WIK-Consult report

Study for the Federal Network Agency Germany

Competitive conditions on transit and peering markets

Implications for European digital sovereignty

Final report

Authors:
Dr. Karl-Heinz Neumann
Dr. Lukas Wiewiorra
Dajan Baischew
Peter Kroon
with the collaboration of
Philipp Thoste

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef

Bad Honnef, 28.02.2022

Imprint

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Germany
Phone: +49 2224 9225-0
Fax: +49 2224 9225-63
eMail: info@wik-consult.com
www.wik-consult.com

Person authorised to sign on behalf of the organisation

General Manager	Dr Cara Schwarz-Schilling
Director	Alex Kalevi Dieke
Director Head of Department Networks and Costs	Dr Thomas Plückebaum
Director Head of Department Regulation and Competition	Dr Bernd Sörries
Head of Administration	Karl-Hubert Strüver
Chairperson of the Supervisory Board	Dr Daniela Brönstrup
Registered at	Amtsgericht Siegburg, HRB 7043
Tax No.	222/5751/0926
VAT-ID	DE 329 763 261

Table of contents

List of figures

List of tables

Executive Summary

1. Building on BEREC's analysis of IP interconnection in 2017, this study aims to elaborate on the trends and competitive developments in this market over the last five years and also to identify emerging trends in the coming years. The study is based on a comprehensive analysis of the relevant literature, evaluations of the PeeringDB, interviews with selected stakeholders, an online survey of IRG members and interviews with selected NRAs.

Developments and trends in IP traffic

2. The volume of IP traffic continues to grow. The trend of declining annual growth rates observed by BEREC has turned into a trend of stable annual growth rates of 22% in Western Europe and 27% in Central and Eastern Europe.

3. The COVID19 pandemic caused a relatively sudden increase in IP traffic. This exogenous shock caused traffic increases of 20 to 30% within days, with a wide dispersion within and between countries. There are indications of a normalisation of annual growth rates at higher levels. However, the sustainability of these trends cannot be reliably assessed at present.

4. Drivers of traffic growth continue to be video streaming and now cloud services as well. While video streaming does not account for 80% of traffic in 2020, as BEREC had expected in 2017, a share of around 80% of traffic comes from the three segments of video, social media and video games. The switch to standard definition (SD) during the pandemic temporarily slowed the growth of video streaming traffic. Otherwise, we continue to expect above-average growth in traffic from video streaming.

5. Even though the proportion of customers demanding symmetrical broadband products is steadily increasing (but still at a low level), the asymmetry of traffic has continued to increase for now. However, the pandemic has reversed this trend. As a result of home office use and especially the drastic increase (+300%) in video conferencing, the asymmetry of traffic has declined from about 1:10 to about 1:9. The sustainability of this trend reversal remains to be seen.

6. Internet traffic has become more and more concentrated in a few sources. Meanwhile, 5-6 players account for well over 50% of all traffic.

7. As a result of the further increase in the meshing of the internet, direct bilateral peering has continued to grow. Thus, the shift from transit traffic to peering traffic continues. Transit is also under pressure from the strong shifts to on-net CDN traffic, which is increasing more than traffic exchange via peering and transit.

8. On a (purely) financial level, peering and transit are comparable interconnection products. While transit essentially incurs variable (traffic) costs, peering incurs fixed stepwise (investment) costs, which are thus degressive per Mbps. However, peering, via a direct connection between parties, has a significantly better (and measurable) quality profile than transit,[1] albeit with a smaller scope of services (only routes and addressable destinations within the other network). Peering and transit are thus not perfect substitutes and can be used complementarily to each other. Whether peering and transit are interchangeable interconnection products cannot be decided in general, but only in individual cases. The competitive relationships of peering and transit are interwoven. A peering (sub)market functions as a competitive market if and as long as ISPs can choose between different transit providers, and thus the transit (sub)market is competitive. Only if substitution is possible is switching to transit a valid alternative when peering negotiations falter. However, because of the qualitative advantages, it is true in any case that peering is a substitute for transit rather than transit being a substitute for peering when it comes to the accessibility of the customers of a particular ISP network.

9. Contrary to BEREC's expectations in 2017, the relative importance of traffic exchange via Internet Exchange Points (IXP) has not increased, but decreased, despite further growth in traffic. In Germany, around 25% (or less) of traffic is still exchanged via DE-CIX. Nevertheless, the importance of IXPs remains central to the functioning of the internet. Smaller players in particular rely on public peering at IXPs. In recent years, IXPs have been more exposed to competitive pressure from data centre service providers who can offer their users low-cost options for bilateral interconnection via cross-connects in addition to classic collocation.

10. The tendency towards a stronger regionalisation of IP traffic, already noted by BEREC, has intensified even further. The ever-increasing processing of traffic via (on-net) Content Distribution Network (CDN) servers has been a major driver of this trend.

11. CDN traffic, and especially on-net CDN traffic, is becoming increasingly important. Globally, it almost tripled from 2017 to 2020 and will double again by 2022, according to expert estimates. On-net CDN traffic comes at the expense of peering and transit traffic.

1 BEREC (2012a): "If two operators mutually agree to exchange traffic on a peering basis this induces lower latency than traffic which otherwise would have to be routed via a transit provider before being handed over to the peer. Peering may also allow ISPs to have greater control over the routing path and performance of traffic. If a poor performance path is preferred by the routing protocols, an alternative path can be configured."

Developments in prices and costs

12. The costs of the network components used for peering and transit continue to fall steadily. The measurable price development of transit and IXP services seems to correspond to the degree of cost reduction of the network components.

13. For IP interconnection, the bill & keep approach continues to dominate. The charging of transit and peering, as far as this is charged, is capacity-based at the point of interconnection (POI). There is no known ISP in Europe that charges traffic-based network fees for internet traffic.

14. South Korea is the only country so far that has responded to the concerns of telcos and introduced the Sending Party Network Pays (SPNP) billing principle on a legal basis. Initially, only ISPs were obliged to exchange traffic with each other as transit for a fee. Subsequently, CAPs were also obliged to pay network charges to ISPs. The implementation of the new rules was and is highly controversial in Korea and is still being fought out in court. Initially, it was mainly national CAPs that were affected. Large CAPs evade this regulation or pay. Market observers report a decline in diversity of online content and expect rising prices for end users for content, as well as lower network infrastructure investments. Quality for end users is declining.

15. The trend towards falling transit prices has continued steadily. While one Mbps of transit traffic still costed USD 0.63 in 2015, it is now less than USD 0.20 and in many cases less than USD 0.10. In recent years, prices have fallen by an average of 20% p.a. Falling prices were and are driven by technical progress and competition in the transit market as well as by peering and on-net CDNs. Prices are still strongly dispersed around the respective averages. Smaller market players benefit less from the low market price level.

16. The peering policy of ISPs and CAPs is transparent to only a limited extent. Many CAPs operate an open peering policy and have only few prerequisites for peering, which, incidentally, is usually settlement-free. Many ISPs have a much more restrictive peering policy, with many requirements for a number of parameters. Deutsche Telekom peers only with Tier 1 backbone operators. It only offers transit to CAPs and does not allow any on-net CDN servers.

17. Our analysis of the PeeringDB database for the German market has led to the following findings about the peering behaviour of important ISPs and CAPs:

    - Akamai's and Facebook's CDNs each have more peering locations than Deutsche Telekom and also higher reported (inbound and outbound) traffic volumes.

- Even regional ISPs with relatively low traffic volumes have a large number of peering sites.
- Telefonica Deutschland and Akamai show surprisingly balanced traffic. Other German network operators have predominantly inbound data traffic, which is due to the asymmetric customer structure (predominantly "consuming" end users).
- While most peering providers prefer multiple handover points, few make this a requirement of peering.
- Among the ISPs and CAPs active in the German peering market, only Deutsche Telekom requires a certain ratio of inbound to outbound traffic.

18. There is still no data (with the exception of France) on the traffic volume of paid peering. According to the CAPs, this is supposed to be the exception in Europe. The traffic-based prices of paid peering are also not very transparent. They seem to range from a few cents per Mbps to a few euros. In any case, they are supposed to be lower than the prices for public peering.

19. According to a price comparison conducted by ACM and updated by us, monthly 10 GE/Gbps port prices at major European IXPs fluctuate around an average of 611€ and for a 100 GE/Gbps port of 3.035€.

Market position of the actors

20. The central asset of the end-user ISPs in relation to the CAPs is and remains the subscriber network and thus the network access to the end customers via their broadband connection. Despite their own TV/VoD and cloud business, the ISPs only compete with the CAPs to a limited extent or, if they are in direct competition, they have the weaker competitive position. This becomes clear in the case of cloud services, for example.

21. As a result of the decrease in hierarchical structure and increase in meshing of the internet, as well as the increasing development and expansion of their own international backbones by the large CAPs, the business model of transit providers and the transit business itself are coming under increasing pressure. Direct peering is increasingly substituting for transit. Above all, however, CDNs and especially on-net CDNs are substituting the business of backbone ISPs. In 2016, CAPs already accounted for a larger share of international backbone capacity than internet backbone providers. Today, the large CAPs only have to reach a small fraction of the autonomous systems (AS)[2] via transit.

2 Wikipedia: An autonomous system is then a system that presents itself to other autonomous systems as if it had only one internal routing plan to give a consistent picture of what destinations (e.g. other networks) can be reached by that system.

22. CAPs have once again increased their investments in transport and delivery infrastructure in recent years in order to handle traffic more efficiently, to reduce dependency on others, to gain more flexibility for their own capacity upgrades and to improve the quality of their service provision to the end customer. In particular, their investments in the delivery infrastructure of CDNs make them much more independent from the network investment decisions of ISPs. In our view, on-net CDNs are an expression of an efficient overall optimisation of the hosting, transport, content delivery and access network infrastructure. The network access provided by the ISP remains as the last bottleneck over which CAPs have no control. However, there are no discernible indications that they will integrate into this level of the value chain as well. Only Google is known to have some small-scale fibre pilot projects of its own in the USA.

23. CAPs operate an open peering policy, do not charge for peering themselves and, according to their own statements, only pay in exceptional cases.[3] The interaction of the networks today - at least on the part of a large proportion of the players - is intensive and cooperative, so that especially in view of the dynamic CDN developments, the question of the payment of network charges seems to have lost relative importance. It remains to be seen how intensively current policy initiatives on the question of payment of network charges to ISPs by CAPs will be pursued.

24. There have been significant shifts in the CDN market in recent years. All major CAPs now operate their own CDNs and place little reliance on the offerings of specialised CDN providers. Netflix's CDN Open Connect delivers (approximately) 100% of Netflix's traffic and content. For the large CAPs, the advantages of integration of the CDN function and having full control over their own CDN have apparently dominated the resilience benefits of a multi-vendor strategy. In light of this tendency towards in-house CDNs, the CDN business of specialised CDN providers has developed less strongly than CDN traffic as a whole. Without being altogether transparent, there is clear evidence that the Internet access providers and carriers have not been able to develop a successful in-house CDN business. In contrast, some of the large CAPs have also developed their own (successful) commercial CDN business.

25. IXP operators have lost relative importance as exchange nodes for IP traffic. Instead, they are increasingly taking on the role of a provider of back-up or resilience for the major players (CAPs, ISPs). They cover traffic peaks, take over surprising traffic loads and take over traffic in case of failure of private peering connections. IXPs are adapting to market trends and changes through the following strategic adaptations:

---

3 There is no single definition; an open policy usually means that anyone can peer, a selective policy has (usually disclosed) criteria that must be met. Parties with a restrictive policy accept only a few peering parties.

- Establishing and expanding their own regional/local nodes,
- Acquisition of new customers through direct contact with large companies,
- Developing their own cloud business,
- Stronger internationalisation of their own business.

Factors influencing market development

26. The most significant technological changes for peering and transit are related to CDNs. Their decentralised location and performance have permanently changed the structure of internet traffic. Further development advances based on artificial intelligence can be foreseen here, which will make the use of CDNs even more attractive. CAPs also cooperate with telcos and equipment manufacturers in the further development of network technologies, e.g. SDN switching platforms.

27. The massive development and expansion of their own backbone and delivery infrastructures by the CAPs has permanently changed the overall global architecture of the internet and the structure of IP interconnection. The architecture has become more meshed and less hierarchical. As a result, the Tier 1 operators are increasingly becoming resilience and back-up providers.

28. Moore's Law still applies to the cost of essential elements of the Internet's hosting transport and delivery infrastructure. With each new generation of equipment, unit cost decreases significantly. Furthermore, the relevant product life cycles are becoming shorter and shorter. This dynamic continues to generate increasing economies of scale. This creates competitive disadvantages for smaller ISPs/CAPs.

29. The sustained growth of internet traffic continues to shape the dynamics of the internet's architecture. In terms of services, the biggest impact comes from the continued disproportionate growth of video streaming and cloud services. At the same time, the architecture of the internet was elastic enough to cope with the sudden pandemic-related traffic increases without noticeable major disruptions.

30. The legal and regulatory framework for IP interconnection has changed relatively little in recent years. With the exception of South Korea, the market for interconnection is unregulated in all countries, i.e. with regard to the conditions of interconnection. However, in a few cases there have been disputes between market participants and, in some cases, intrusions by NRAs into the contractual freedom of market players. Indirectly, there is also a connection between the net neutrality rules that have been in force in the EU since 2015 and the wholesale level, because a disruption of interconnection at the wholesale level can also lead to end users not reaching all destinations of the internet, with lasting implications for net neutrality.

31. In two merger decisions, the EU Commission has made it clear by imposing remedies that they will take steps against (potential) abuse in peering and transit resulting from an integrated business model of ISP business and content business.

IP interconnection disputes

32. There were only a few cases of direct regulatory intervention in the peering and transit markets in Europe during the period under review. This is also confirmed by the IRG survey. The best known case is the protracted peering dispute between the backbone ISP Init7 and the telco incumbent Swisscom in Switzerland. This may also be due to the lack of transparency as regards interconnection disputes.

33. In the Init7/Swisscom case, the view of the Swiss competition authority that Swisscom had exploited its dominant position in peering to the detriment of Init7 was confirmed by the highest court in April 2020. Furthermore, the Federal Administrative Court stated that IP transit is not a substitute for peering, and that traffic asymmetry cannot constitute a price criterion for peering. It is now up to the regulatory authority to set cost-oriented prices for peering.

34. A spectacular case of turbulence in internet traffic occurred due to a re-routing decision by T-Mobile NL. T-Mobile withdrew from the IXP AMS-IX in October 2019 and routed all traffic via Germany. This left many small online providers, as well as cities and municipalities, cut off from traffic exchange. Unlike the large CAPs, they could not switch to peering contracts. After a fierce public reaction, T-Mobile returned to the previous status quo.

How has the relative power structure of the actors changed?

35. The relationship between CDNs and ISPs has changed significantly in recent years. This applies both to vertically integrated in-house CDNs of the large CAPs and to commercial CDNs. Whereas CDNs exchanged their traffic with ISPs across network boundaries (peering or transit) ten years ago, on-net exchange now predominates, with the CDNs' cache servers collocated directly in the ISPs' networks. Only a few ISPs do not allow on-net data exchange, continuing instead to exchange traffic across network boundaries and POIs. However, CAPs only offer on-net caching for a minimum volume of data exchange with an ISP. In this respect, the interconnection profile between CDNs and ISPs has changed completely. Besides quality gains, there are efficiency gains from on-net caching (less data traffic). These apply to both CAPs/CDNs (less traffic to be backhauled) and ISPs (less traffic in the core network).

36. Ten years ago, CAPs still used the services of (pure) CDNs on a large scale. This has changed fundamentally insofar as the large CAPs have all integrated the value creation stage of the CDNs, i.e. they all operate their own CDN optimised to their respective needs for handling their traffic. In this respect, the customer structure and therefore also the data volume transported by pure CDNs has changed. At the same time, some CAPs have built up their own business in the area of CDN and cloud services. In this respect, value creation has also shifted towards the CAPs.

37. The CAPs' investments in their own backbones and in decentralised (on-net) CDNs has permanently changed the classic two-sided market relationship between ISPs and CAPs for large parts of the market. The ISPs' networks are no longer the unilateral platform through which the CAPs bring their content-based services to the end user. CAPs now have their own (network) platforms for essential elements of the transport value chain. In the on-net CDN model, (parts of) the network platform are planned and delivered cooperatively. Nevertheless, ISPs remain responsible for end-user quality including the management of CAPs' cache servers in their networks. The significant investment of CAPs in their own network infrastructure has not changed the ISPs' access monopoly for their end-users, but it has allowed CAPs to increase the end-user quality of their services. One can interpret this shift as a shift of value creation from the ISPs to the CAPs. At the same time, it has also made the relationship between CAPs and ISPs more cooperative. They now exercise more of a joint role in determining the quality of service to be delivered. For large ISPs that do not allow on-net caching, on the other hand, little has changed in the classic model of the two-sided market.

38. The cloud business has developed particularly dynamically in the last five years. The large cloud providers offer cloud services not only to business customers, but also to large CAPs such as Netflix, Apple and Spotify. They are responsible for significant parts of the IP traffic. They largely rely on their own backbones and only request limited transit services from backbone ISPs. The offering of cloud services by cloud providers to business customers is in direct competition with cloud services offered by ISPs. The public cloud market is dominated by Amazon, Google, IBM and Microsoft.

39. The large cloud providers have to some extent overtaken the backbone ISPs as the backbone of the internet. Through their interconnected infrastructure, they have contributed significantly to the meshing and the flatter hierarchy of the internet. They can bypass the Tier 1 ISPs with their own networks to a substantial degree, and are largely independent of them. This increasing interconnectivity of a few large networks has contributed to the decline in transit revenues of the Tier 1 operators. The large cloud providers have largely replaced the backbone operators as the principal carriers of internet traffic.

Introduction

Aim and scope of the study

The internet was originally designed as a decentralised network that is resistant to disturbances and failures due to its structure. Due to the internet's meshed topology, data packets can reach their destination through the network via different routes. The individual network components (e.g. routers, switches) are designed to act as autonomously as possible, to process data packets in sequence and to forward them to the best-performing downstream network node in the direction of the destination.

The quality of a data transmission in the internet is therefore significantly influenced by the capacity of network transfer points and nodes. The fewer transfer points and resources there are between network sections, the fewer possible routes there are for a data stream between source and destination. Particularly in times of steadily increasing transmission volumes, data transmission is increasingly vulnerable to possible capacity bottlenecks at peak times or in the event of failures. However, this is offset by lower risks of failure due to a stronger meshing of the internet.

The connection between networks (Autonomous Systems) of different operators takes place both by peering agreements and via transit connections. Commercial transit providers typically offer their customers access to or reachability for the entire internet. In contrast, peering only grants mutual data exchange between the networks of the parties involved (and to their respective customers who are connected to those networks). In order to avoid transit costs and/or to increase the quality of network interconnection through peering, network operators can interconnect (peer) either at public internet exchanges or directly with one another. A bilateral "settlement-free"/"bill-and-keep" peering agreement is usually based on the premise that the traffic volume between incoming and outgoing data traffic is balanced between the two partners and that no charge therefore flows for the traffic exchange.

With the popularity of over-the-top audio and video streaming services, end-users in particular are creating an increasingly asymmetric flow of data between their ISPs' networks and their interconnection partners, who primarily pass this content through. The popular content and service providers (CAPs) notably include Netflix, Google and Facebook, which account for a large share of the data traffic to end customers.

The increasing asymmetry can lead to the conditions for settlement-free peering being fulfilled less and less often, even in the case of economically balanced partners. So-called "paid peering" has now established itself on the market as an option to reflect asymmetries in the economic agreements between network operators. In the case of paid peering, the costs for peering are primarily imposed on the partner that sends more traffic into the network of its interconnection partner than it receives. In addition, it is possible to demand monetary compensation for direct peering that is higher than the costs of the actual interconnection (feed-in, server, switches, rent, electricity, etc.). This may be due to the fact that the connection achieves a higher quality level (jitter, delay, packet loss) through direct peering than would be possible via a transit provider available in the region concerned. In addition, direct peering leads to a reduction in transit costs for both providers, as only the residual data traffic that cannot be handled via peering has to be routed via a transit provider. Furthermore, direct interconnection with high quality can make the integration of a content distribution network (CDN) independent of the CAP less relevant or even superfluous. Therefore, the larger a CAP is, the more likely it is to integrate along the value chain. Thus, CAPs establish their own hosting capacities, develop their own network infrastructure or operate a CDN themselves.

As intermediaries, CDN operators store popular content from CAPs in geographically distributed server architectures and thus minimise the distance between end customers and the storage location of the content. This also reduces the distance relevant for data transmission to the end customer, thus avoiding a large number of (potentially busy) nodes and paths and increasing transmission quality.

In this area of tension, the latest BEREC Report on IP Interconnection of 2017[4] identified the following trends in the industry compared to the situation that had existed at the time of the previous study of 2012:

- The transmitted data volumes had continued to increase, driven by the popularity of OTT offers from the streaming segment.
- The market was increasingly relying on the use of CDNs, interconnection at internet nodes, and direct interconnection.
- Prices for transit and CDN services had continued to fall over the same period.
- The relative relevance of transit as opposed to the other available options had therefore decreased.
- In contrast, paid peering had clearly increased in importance during the observation period.

These developments mean that the formerly decentralised structure of the internet is increasingly characterised by a small number of bilateral relationships at the Network Layer and central intermediaries (especially CDN services) at the logical networking layers above. However, with the world's largest websites and services clustered around a few large infrastructure providers, commercial disputes between interconnection partners and failures of CDN infrastructures can have far-reaching implications for the accessibility and quality of internet services experienced by consumers.

4 BEREC (2017).

Against this background, the Federal Network Agency commissioned the present study. In this study, the forecasts and economic conclusions of the BEREC study (2017) were to be taken up, validated and supplemented by further subjects of investigation, in particular aspects of digital sovereignty. In particular, the market and competitive trends in this market over the last five years were to be worked out in more detail and the emerging trends of the next few years were also to be identified.

Research approach

In addition to the evaluation of a number of studies with direct and indirect reference to the topic that WIK conducted, this study is based on the following research activities:

- Literature review,
- Interviews with selected stakeholders,
- Targeted evaluation of a subset of the PeeringDB database,
- Online survey of European NRAs via the Independent Regulators' Group platform,
- Interviews with selected NRAs.

In our desk research and literature review, we included relevant publicly available reports, studies, publications by authorities and institutions as well as scientific publications, to the extent that they were published after 2017. In total, we evaluated more than 100 documents.

In order to validate our preliminary assessments, to gain more in-depth indications in an overall informal and non-transparent environment and assessments and evaluations of important players for market events, we interviewed representatives of selected stakeholders. Interviews were conducted with Facebook, Google, Netflix, Init7, Deutsche Telekom and DE-CIX. In each of the interviews, experts from different company divisions were available to us. There were always experts present who were responsible for the company’s own networks and for the interconnection with other networks. In some cases, the interview partners provided us with additional written documents.

We only selectively evaluated data from the complex PeeringDB. Our specific evaluation focus was on peering and on peering policy for the German market.

In order to gain insight into the spectrum of views across Europe on IP traffic development, pricing trends, but above all on IP interconnection disputes and the involvement of regulators, we conducted an online survey (with a total of 45 questions) among all members of the IRG. The results of this survey are presented in the appendix to this study and otherwise directly incorporated into the study.

In order to go into more detail on selected aspects of the opinions of individual IRG members, we conducted in-depth interviews with the Dutch regulatory and competition authority ACM and with the Finnish authority Traficom as a follow-up to the online survey.

Structure of the study

The first two chapters focus on the development of market conditions. In Chapter 1, we trace the development of transport in the dimensions of growth, services, symmetry, concentration, peering vs. transit, regionalisation as well as via specific provider groups.

It should be noted that the period from 2020 onwards was significantly influenced by the COVID-19 pandemic. This means that recurring periods of lockdowns, obligations to work from home, and general contact restrictions have significantly influenced consumer behaviour ass regards internet use. This implies that recent developments in consumer behaviour should not necessarily be seen as a trend, but rather as an exogenous shock. When extrapolating based on historical data of the recent past, it is therefore questionable whether the years 2020/21 provide a reliable view into the further development of the interconnection markets. Even if it can be assumed that teleworking and video streaming will remain at a comparatively high level compared to the time prior to the pandemic, a declining trend can initially be expected here in the foreseeable future.

In Chapter 2, we look at prices and price trends for the various forms of IP interconnection. Here we also examine current developments in pricing and billing principles.

In Chapter 3, we explore the market position of key stakeholder groups and its determinants. We shed light on their motivations to invest in their own infrastructures and to choose between the different forms of interconnection. Within the framework of a stakeholder approach, the interdependencies and payment flows between the groups of actors involved in transport exchange and their strategic developments are examined.

In Chapter 4, we work out the central factors influencing market development. Which factors drive the developments identified in the peering and transit markets? We examine the contribution of technological changes, changes in network structures, prices and costs, traffic and services, and changes in the legal and regulatory framework.

Chapter 5 focuses on the analysis of the observed shifts in the relative power structure of the main groups of actors and market players. Has the relative market power changed in such a way that the market balance in transit and peering has changed? We also briefly review the available evidence we have collected on IP interconnection disputes.

In Chapter 6, we review the relevant dimensions of digital sovereignty and discuss the specific implications for digital sovereignty from the developments described in the IP peering and transit markets.

1 Developments and trends in IP traffic

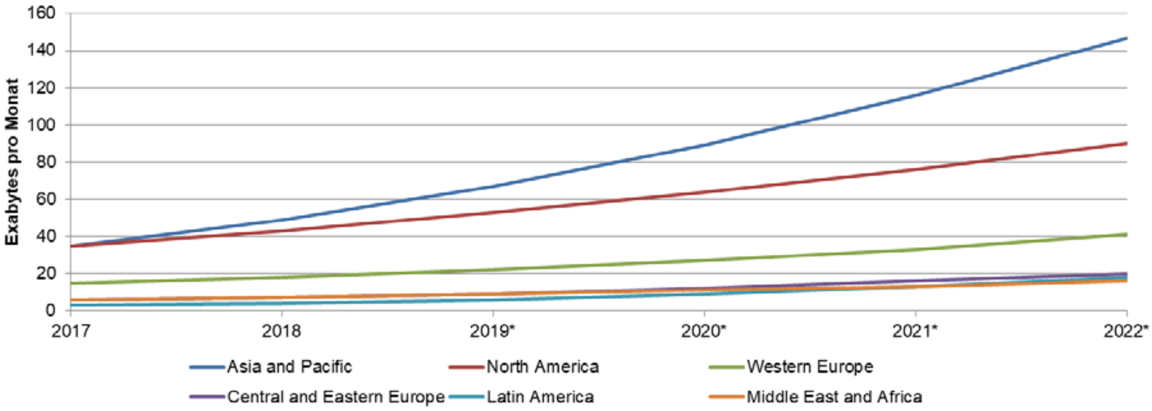
1.1 Traffic growth

The BEREC Report[5] 2017 found that (fixed) internet traffic volumes have continued to grow since 2012, but at a declining annual rate of around 20% for Western Europe and 27% for Central and Eastern Europe (CAGR 2015-2020).

According to recent studies, global data traffic via the internet (fixed network) continues to grow. Cisco forecasts an annual CAGR of 27% between 2017 and 2022. A particularly strong increase is expected in the Latin America region, with an annual CAGR of almost 43% over the years 2017-2022. Similarly, a particularly strong increase is expected in the Asia and Pacific region, where an annual CAGR of 33% is estimated over the years 2017 to 2022. The declining rate of increase is not continuing in Europe, where the growth rate is stagnating. For the same period, traffic volumes in the Western Europe region are expected to grow by 22% (annual CAGR), and in Central and Eastern Europe by 27% (annual CAGR) (Figure 1-1).[6]

Thus, the trend of growing data traffic identified in the BEREC Report[7] 2017 continues globally for the time being, but with growth rates for Europe that are no longer falling, but rather constant.

Figure 1-1: Global consumer IP traffic data volumes from 2017 to 2022, by region

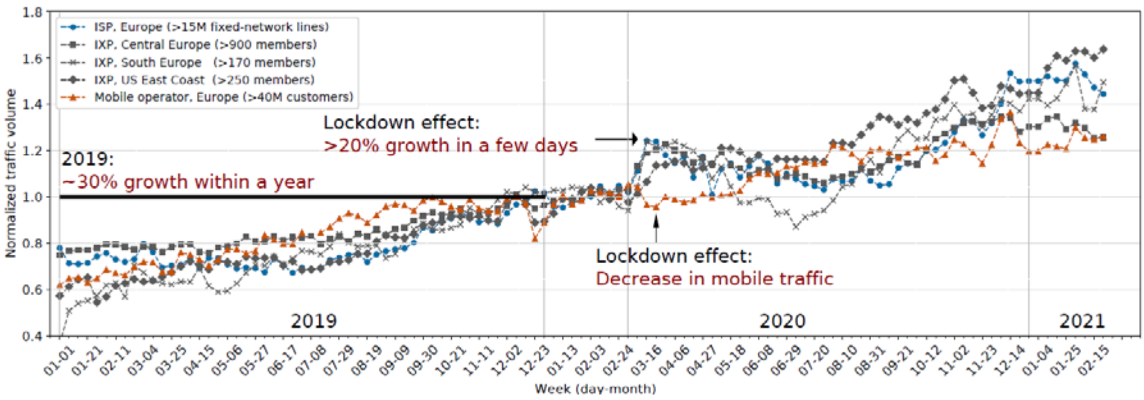


Source: Cisco VNI 2018 (2019), https://www.statista.com/statistics/267199/global-consumer-internet-traffic-by-region/. *Forecast.

5 BEREC (2017).
6 Cisco (2019).
7 BEREC (2017).

This relatively steady and stable growth trend has received an exogenous shock from the social and economic implications of the COVID-19 pandemic. Restrictions on public life during the COVID-19 pandemic resulted in a sudden and unpredictable shift in user behaviour, which also changed the way internet products are consumed and used. A sudden increase in traffic is evident in Figure 1-2, which shows a lockdown effect of data traffic of over 20% within a few days. During the spring of 2020, this effect could also be seen at DE-CIX in Frankfurt as shown in Figure 1-15. An opposite effect could be observed with the mobile network operator shown (Figure 1-2), whose traffic volume decreased as a result of the lockdown measures.

Figure 1-2: Development of data volume before and during the Corona pandemic based on an ISP and selected IXPs



Source: Feldmann et al. (2021, p. 3).

Feldmann et al. (2021) describe, beyond the increased data traffic, both a shift in the usual behaviour towards a more even use throughout the day and a shift in the services predominantly used. The latter in particular has an impact on the peering issue, as uploads have become more relevant with the increased relevance of video communication services.

Another study of Facebook server utilisation from 2020 shows that the pandemic first caused a sharp increase in traffic volume, but this was limited to a short period of time. This increase was followed by a period of increased but stable traffic volume. The initial increase in traffic showed regional differences, both in terms of timing and growth. This is due to the different lockdown regimes and timing.[8]

In the survey of IRG members, the vast majority report an increase in IP traffic in their respective countries (91%); 73% even report a strong increase.

8 Böttger et al. (2020), p. 1.

The COVID-19-induced increase in internet traffic is also evident in the traffic figures for France. In its regular reporting on the development of the internet, ARCEP reports a 50.4% increase in (inbound) traffic from the end of 2019 to the end of 2020.[9] The year before, the growth rate was still 29%.[10]

Deutsche Telekom also reports high growth rates of IP traffic until 2020 (from 2018 to 2019, the growth rate in Germany was about 20%). After that, growth is stable, which is explained by a relative market saturation for streaming services that occurred in the meantime. The traffic boost that occurred in France due to COVID-19 cannot be observed in the same way in Germany according to Deutsche Telekom's observations. Although traffic still rose sharply in Q4/2019, it fell again in March 2020 as a result of the Breton initiative to reduce the resolution of video services (from HD to SD). The classic seasonal traffic patterns seem to dominate the COVID 19 influence again.

1.2 Structure of the traffic

1.2.1 Services that drive traffic growth

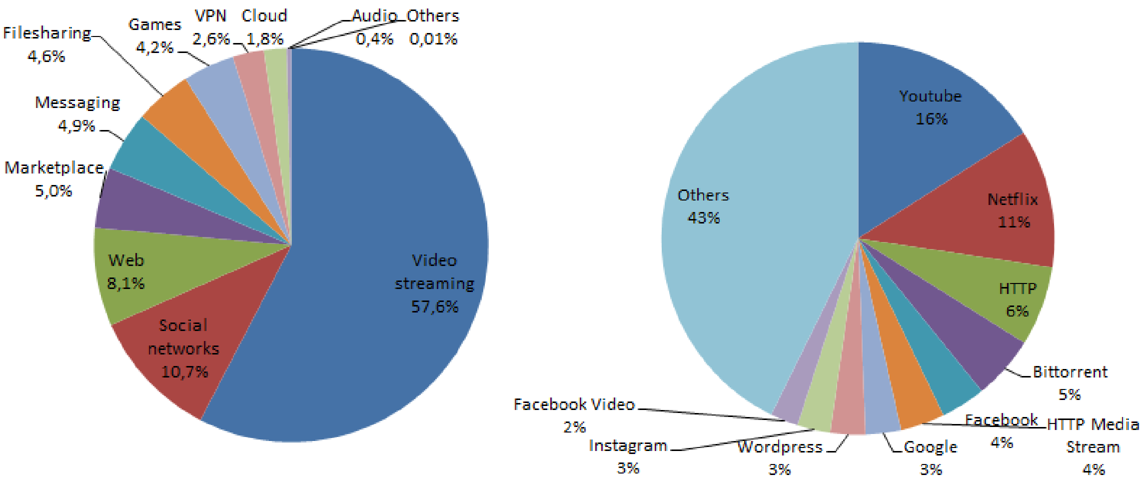
The 2017 BEREC Report noted that increasing data traffic was largely driven by video streaming services; this was expected to rise from 66% in 2015 to a projected 83% in 2020 for Western Europe. In addition, internet traffic via mobile and WiFi devices was expected to grow in importance, rising from 62% in 2015 to 78% in 2020.[11]

Video streaming indeed continues to take a significant share of IP traffic. However, video streaming did not reach an 80% share of total IP traffic. According to Sandvine's[12] calculations, the share of the global video streaming segment measured in May 2020 is 57.64%. Global data traffic leaders YouTube (15.94%) and Netflix (11.42%) in first and second place accounting for the most traffic globally. In addition, most major video streaming services (including YouTube and Netflix) changed their regular streaming resolution to standard definition (SD) during the COVID 19 pandemic to counter potential network congestion, so this figure would have been higher for both streaming services had this adjustment not occurred.[13] The video, social sharing (includes social media as well as, for example, pictures and videos stored in the cloud) and video games segments together represent about 80% of all data traffic, according to the study by Sandvine (2020).

9 ARCEP (2021), p. 41.
10 ARCEP (2021), p. 33.
11 BEREC (2017).
12 Sandvine (2020), p. 6.
13 Sandvine (2020), p. 7.

Video games themselves only rank seventh in the global segment rankings, but there was the largest increase in this category compared to 2019, at nearly 48.11%. Although the initial increase in gaming traffic was download traffic, interactive gaming traffic, including cloud gaming services such as GeForce Now and Stadia, increased during the observation period between 2019 and May 2020, driven by changing consumer behaviour at the onset of the COVID-19 pandemic.[14]

Figure 1-3: Composition of global data traffic and apps, May 2020



Source: Sandvine (2020), pp. 6f. The Global Internet Phenomena Report 2020 data comes from over 500 fixed, mobile and WiFi operators worldwide. The report does not include significant data from China or India; however, the data represents 2.5 billion subscribers and thus a statistically significant segment of the internet population (Sandvine (2020), p. 1).

Ahead of YouTube, which has historically been the most popular mobile internet service in terms of traffic, Netflix has emerged as the number one service on landlines during the COVID-19 pandemic.

The great relevance of increasing traffic volumes for video services is also reflected in the ARCEP report, which attributes a combined 50% share of traffic from French ISPs to the companies Netflix, Google, Akamai and Facebook.[15] These companies are either themselves active as CAPs in the field of video services (Netflix, Google with Youtube, Facebook in parts with Facebook and Instagram videos) or, like Akamai, are indirectly involved in the distribution of video services as CDNs.

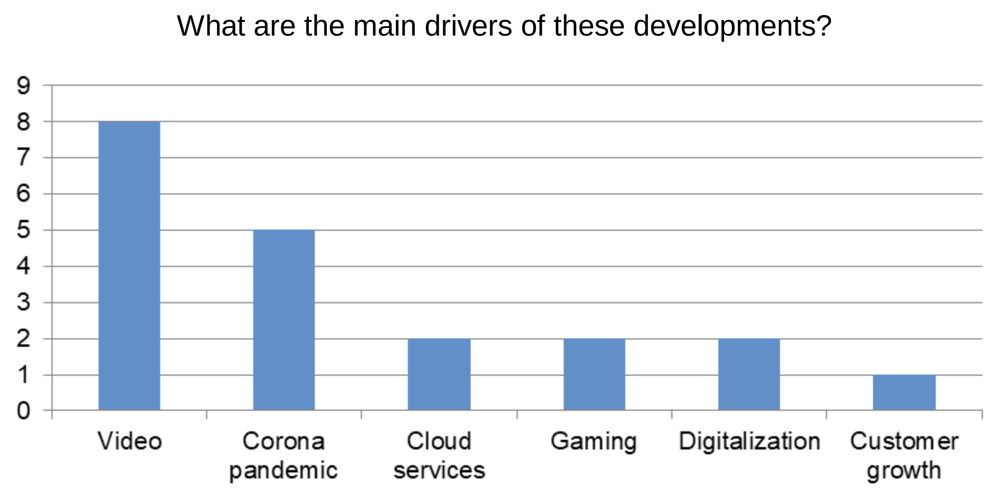
14 Sandvine (2020), p. 6.
15 ARCEP (2021), p. 45.

The increase in the video streaming segment is driven by the growing adoption of high-definition video streaming and an increasing number of high-definition TV sets. Compared to standard-definition (SD) video, which requires approximately 2 Mbps of data rate, high-definition (HD) video content requires 5 to 7.2 Mbps and ultra-high-definition (UHD) video content requires 15 to 18 Mbps, a nine-fold increase over SD.[16] These figures are in line with those of Netflix, which recommends 3 Mbps (SD), 5 Mbps (HD) and 25 Mbps (UHD) connection speeds for its services.[17] At the same time, Cisco projects an annual CAGR of 27% between 2018 and 2023 for high-definition 4K TV sets, which is expected to further drive future traffic volume growth (see Figure 1-6).

WIK's regular monitoring of the use of OTT services also shows a steady increase in internet-based video use.[18] In 2020, 45% of respondents used internet-based video services at least 61% of the time and only 22% used traditional video playback alone. Figure 1-5 shows the development of the use of audiovisual services broken down by provider in the period 2015 to 2020. In this period, the use of Netflix, for example, increased more than sixfold.

Video streaming as a key driver is also confirmed by the IRG survey for this study. For 73% of respondents, this service was the main driver of traffic growth (see Figure 1-4). Cloud services and customer growth trail substantially.

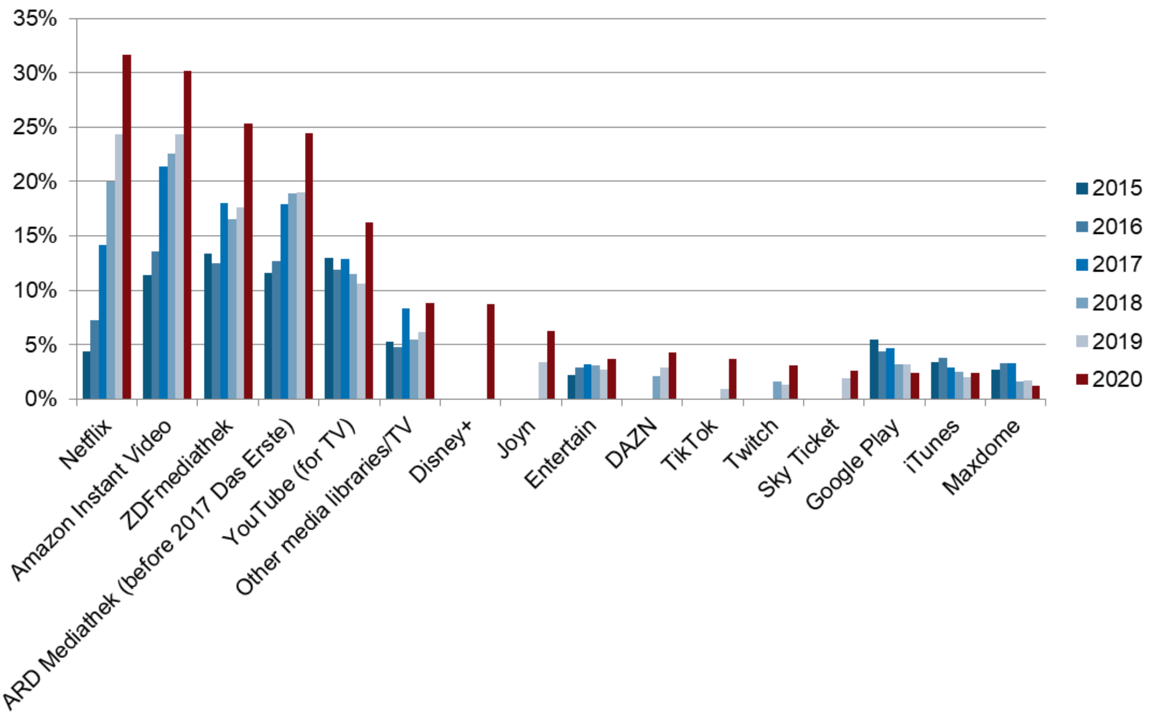
Figure 1-4 Drivers of traffic growth



Source: WIK-IRG online survey.

16 Cisco (2020), see also Figure 1-6.
17 https://help.netflix.com/de/node/306.
18 Data based on an annual WIK survey in the period 2015 to 2020.

Figure 1-5: Use of audiovisual services by provider in the period 2015 to 2020 (proportion of respondents who used the service in the last month)



Source: Data based on an annual WIK survey in the period 2015 to 2020.

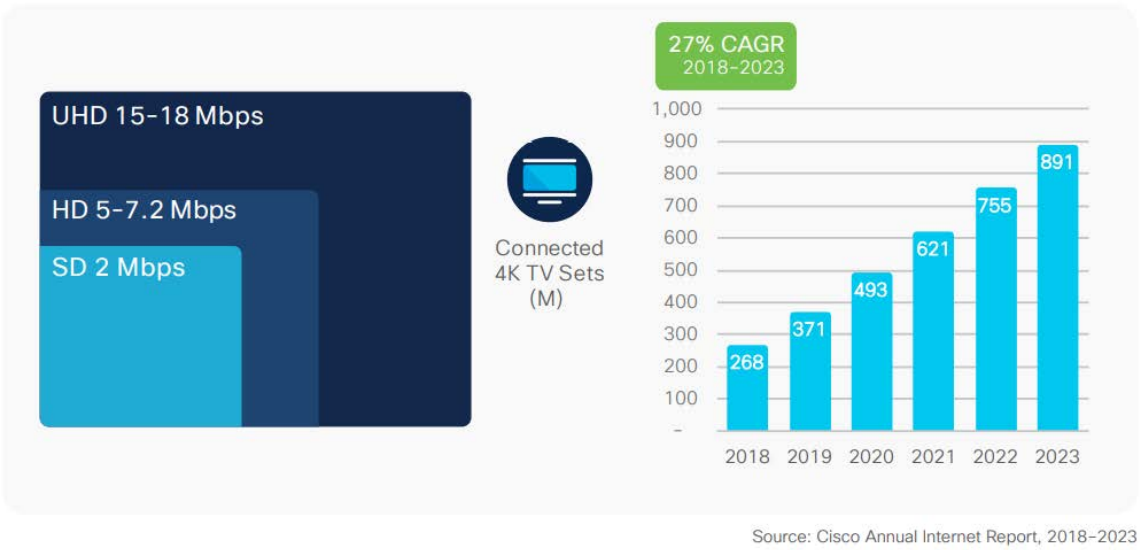
Nevertheless, there is no end in sight to innovative video offerings. The next generation of 360-degree videos with 8K resolution, 90 frames per second and more, High Dynamic Range (HDR) content and stereoscopy (spatial impression of depth) require 50 to 200 Mbps in the downstream direction. In addition, for so-called 6DoF videos (i.e. videos in which the viewer can move in six degrees of freedom), 200 to 5000 Mbps are required.[19] However, codec development is making further progress in parallel, so that relatively less bandwidth is needed for higher resolution. Efficient formats for storing video content (codecs) enable CAPs to store their video content in smaller and smaller files at the same resolution without any significant loss of quality thanks to compression, which in turn has the effect of reducing the volume of data transmitted.

Remote connectivity and interaction through holographic communication or virtual reality (cf. Meta's [formerly Facebook] Metaverse plans), together with all human sensory input information ("Internet of Senses"), will further drive data rates. Multiple cameras to film from different views for holographic communication will require data rates in the order of terabit(s) per second.[20] Therefore, it can be assumed that with the

19 Qualcomm (2018), p. 10.
20 Calvanese Strinati et al. (2019), p. 3.

availability of these technologies on the mass market, the demand for bandwidth will continue to grow. With this in mind, we continue to expect strong growth in traffic demand from video streaming.

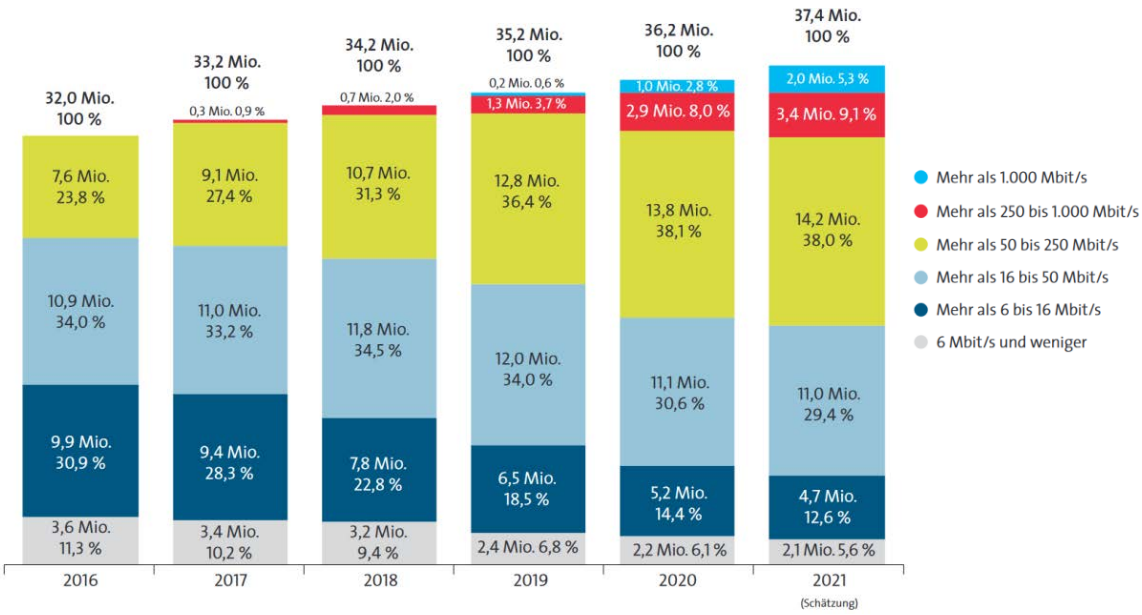
Figure 1-6: Data rates for SD, HD and UHD resolutions and global increase of 4K TV sets



Source: Cisco (2020).

The growth in traffic and the increased demands of consumers are accordingly also reflected in the demand for broadband products in higher broadband classes. According to the VATM's 2021 market analysis, for example, the share of consumer demand for broadband products with speeds of 50 Mbps or more rose from 28.3% to 52.4% between 2017 and 2021. The share of of consumer demand for gigabit broadband products is experiencing particularly strong growth.

Figure 1-7: Consumer demand for broadband products by bandwidth class from 2016 to 2021



Source: Market Study 2021 by VATM and DialogConsult (2021), p. 18.

1.2.2 Symmetry/asymmetry of traffic

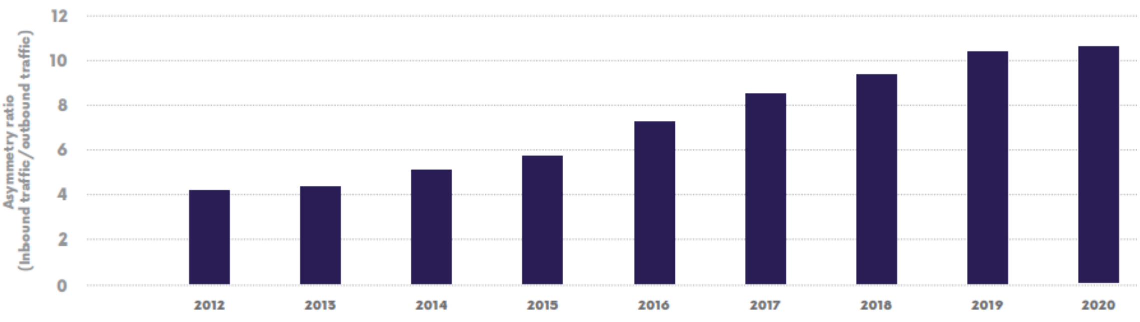
The behaviour and usage profile of internet users has always led to asymmetric traffic flows. In line with this usage behaviour, asymmetric access products continue to dominate the market. Only a small, albeit growing, proportion of broadband customers - usually business customers - currently demand symmetrical access products. In this context, the OECD (2020) reports in its market survey that the importance of less asymmetric broadband products is increasing.

This demand behaviour is reflected in the aggregated traffic flows. However, there are still only a few studies and sources that generate a representative or complete picture of the extent of the asymmetry of traffic.

In France, a growing asymmetry of up- and download traffic can be observed over the years. Inbound (i.e. toward the user) versus outbound traffic are roughly in a ratio of 11 to 1 in France in the second half of 2020. The share of inbound traffic has risen steadily from 1:4 to 1:11 since measurements began in 2012 (see Figure 1-8). However, a different trend is emerging at the current margin. While outbound traffic in France increased by 36% in the first half of 2020, inbound traffic increased by only 26%.[21]

21 ARCEP (2021), P. 42.

Figure 1-8: Asymmetry of traffic between inbound and outbound for the main ISPs in France between 2012 and 2020



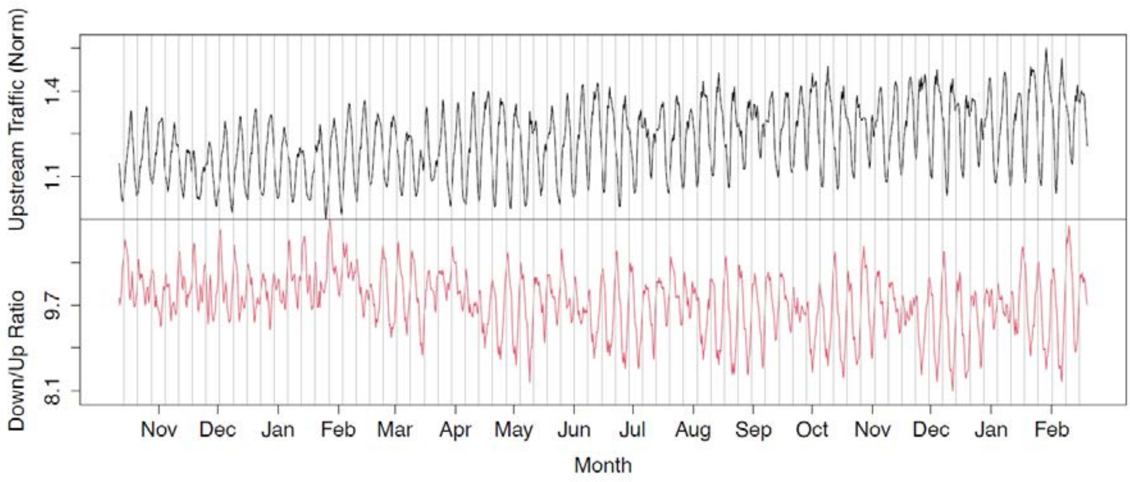
Source: ARCEP (2021).

Similar orders of magnitude on the relation of inbound and outbound traffic can be observed for a not specifically identified European ISP with 15 million customers. The lower part of Figure 1-9 shows an asymmetry with a factor of 9.8 before the COVID-19 pandemic. At the same time, the increase in outgoing data traffic described in Section 1.1 in light of the COVID-19 pandemic reflects the use of less asymmetric services such as videoconferencing versus the highly asymmetric traffic drivers of video streaming services. With the shift of office activities to the home office, this issue became more important, especially from a peering perspective. Video communication requires a low latency, and leads to a less asymmetric ratio of incoming and outgoing traffic. For example, Feldmann et al.[22] found that the 300% increase in the use of video communication services was accompanied by an 18% increase in outgoing traffic above the overall increase in traffic. As a result of this increase, the inbound/outbound factor also decreased from 9.8 to 9.0 in the period from October 2019 to February 2021. This trend as a result of the COVID-19 pandemic is in slight contrast to the previous observation that video streaming services, as very asymmetric services, account for an increasing share of global traffic. However, it remains to be seen which usage behaviour and thus ratio can be expected after the end of the COVID-19 pandemic.

Google also reports that the asymmetry of traffic has decreased somewhat as a result of the COVID-19 pandemic. Services with high upload traffic (e.g. videoconferencing) have grown relatively more than other services during this time.

22 Feldmann et al. (2021), p. 5.

Figure 1-9: Development of upload data traffic compared to the first January week 2020 and the down-to-upload ratio respectively from October 2019 to February 2021



Source: Feldmann et al. (2021), p. 5.

1.2.3 Concentration of traffic

Internet traffic is relatively concentrated in terms of its origin/source. BEREC 2017 makes this trend evident in the number of networks that account for 50% of the traffic. In 2007 this was several thousand networks; in 2009, 150 networks; and in 2013, 35 networks. Although global data for the expected continuation of traffic concentration is only sporadically available, there is clear evidence for a further increase in concentration.

Schlinker et al. report that in 2017, ten ASes were responsible for 70% of the traffic. In 2007, several thousand ASes were responsible for the same share of traffic.[23]

Deutsche Telekom also reports a strong increase in the concentration of traffic of a few players.[24] CDN traffic now accounts for a share of 60-70%. This is predominantly attributable to Google (YouTube), Netflix and Amazon Prime. Although there are always new relevant players as traffic sources, such as TikTok in recent years, the concentration of traffic of 5 or 6 players is constantly increasing.

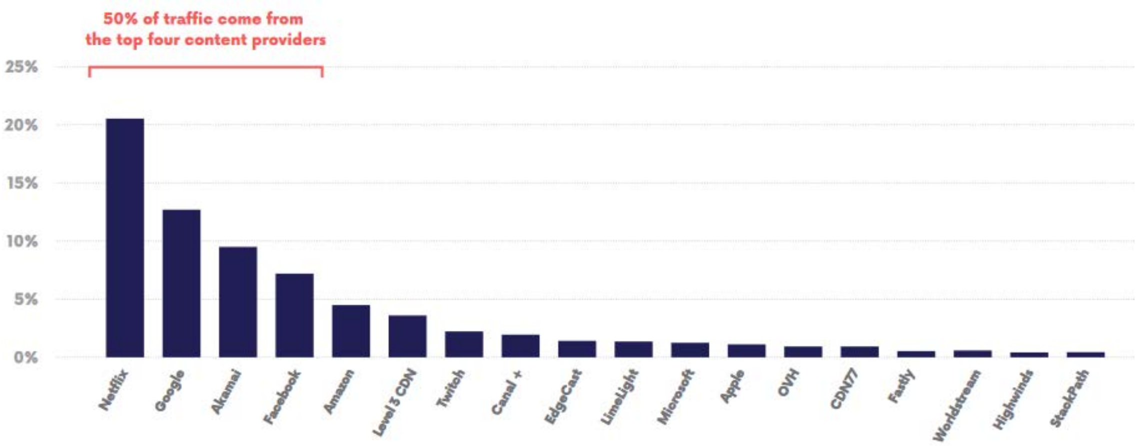
ARCEP also reports that by the end of 2020, more than 50% of the inbound traffic of the main French ISPs was accounted for by the four providers Netflix, Google, Akamai and

23 Schlinker et al. (2017), p. 1.

24 "Five internet corporations cause 50 per cent of all data traffic in Germany, eight over 80 per cent.", https://www.welt.de/wirtschaft/article231167253/Telekom-Chef-Timotheus-Hoettges-Deutschland-steckt-in-einer-Umsetzungskrise.html

Facebook.[25] The density curve in Figure 1-10 becomes much flatter thereafter. These companies are either themselves active as CAPs in the field of video services (Netflix, Google with Youtube, Facebook in part with Facebook videos and Instagram videos) or, like Akamai, are indirectly involved as CDNs in the distribution of video services.

Figure 1-10: Source of end-user traffic of the main ISPs in France (end 2020)



Source: ARCEP (2021).

A lower concentration of the origin of global data traffic is shown by the Sandvine (2020) study, which captures traffic from over 500 fixed, mobile and WiFi operators worldwide (but excluding India and China) (see Figure 1-3).

1.2.4 Peering vs. transit traffic

IP transit is primarily used by networks to reach other networks that would be too expensive to reach by expanding their own network to locations where direct interconnection would be possible. This applies, for example, to a network that only operates within national borders. Such (purely) national networks need a transit provider to reach all other networks on the internet. Typically, as networks grow, they interconnect directly with more networks. According to Facebook's assessment, ISPs in Europe can now handover the (vast) majority of their traffic within their country, so their dependence on transit is significantly reduced.

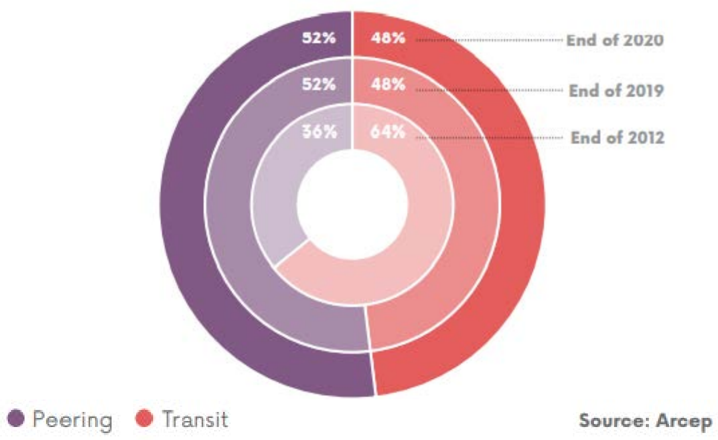
There is little publicly available information on the division of interconnection traffic between transit and peering, and between public and private peering. BEREC expected in 2017 that the relative importance of public peering via IXPs would increase.[26]

25 ARCEP (2021), P. 45.
26 BEREC (2017), P. 11.

Regarding the relative importance of transit, BEREC made reference only to the observation of a decrease of transit relative to (private) peering in France.

This trend has continued in France in recent years. The share of interconnection via (private) peering has progressively increased. While the share of transit was still 64% in 2012, it was only 48% in 2020. However, there has been no further shift in the share in 2020 (see Figure 1-11). ARCEP attributes this absence of growth in peering traffic to a partial substitution of on-net CDN traffic for peering traffic.

Figure 1-11: Change in peering and transit of the main ISPs in France (by inbound traffic volume)



Source: ARCEP (2021), p. 44.

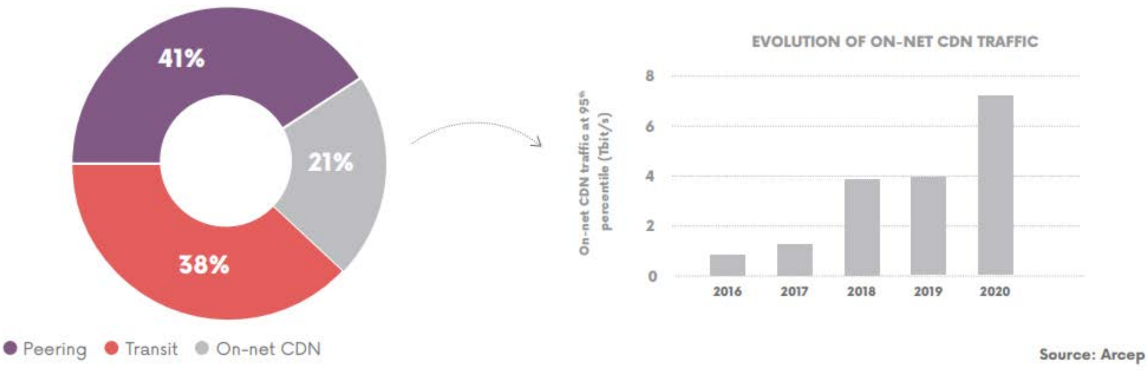
This shift in share is essentially due to the increase in peering capacity between ISPs and the large CAPs.

Public peering remains relatively insignificant in France and accounted for only 2.9% of total inbound traffic at the end of 2020.

Significant shifts have occurred in 2020 in the ratio of on-net CDN traffic to transit and peering. On-net CDN traffic almost doubled in 2020 (+82%) and thus grew much more strongly than peering and transit. The share of on-net CDN traffic has thus risen from 17% to 21% (see Figure 1-12). ARCEP attributes this shift to the changed use of the internet during the COVID-19 pandemic, notably the increased use of VoD services that rely heavily on on-net CDNs in ISP networks.

Deutsche Telekom also reports a relative decrease in transit traffic. Deutsche Telekom does less transit business abroad today than it did a few years ago. Transit business in Europe and Eastern Europe is concentrated in countries in which Deutsche Telekom itself is also active as an end-customer ISP. Deutsche Telekom feels that no solid business model is possible with transit, especially in Asian markets.

Figure 1-12: Breakdown of traffic to customers of the main ISPs in France by interconnection type (end 2020)

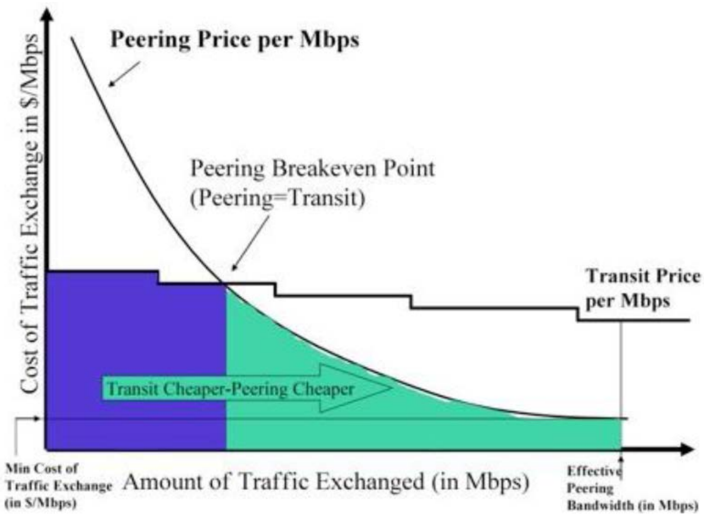


Source: ARCEP (2021), P. 45.

1.2.5 The decision between peering and transit

The decision to choose peering or transit for interconnection with other autonomous systems follows both cost/price and quality considerations and differences between the two forms of interconnection.

Figure 1-13: Peering vs. transit



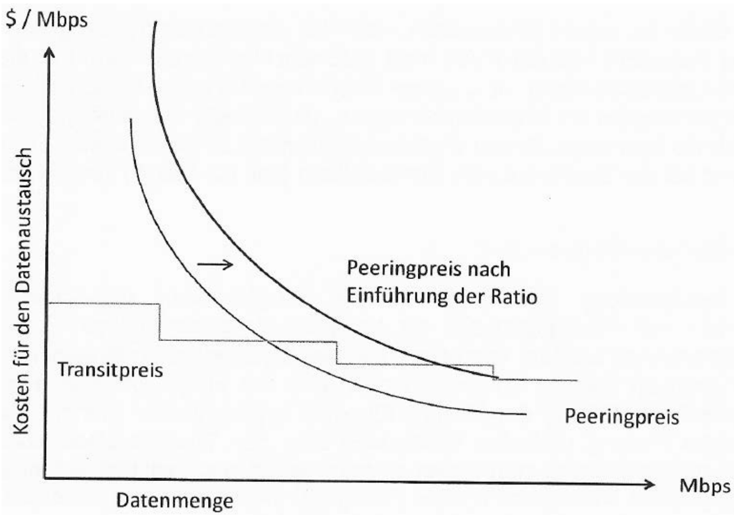
Source: BEREC (2012).

Insofar as the decision between peering and transit in the interconnection between two specific networks is determined by cost/price considerations, it is made on the basis of an opportunity cost calculus. Transit essentially incurs variable costs (per Mbps), whereas the costs of peering are essentially fixed costs and thus show a degressive progression per Mbps (see Figure 1-13). On the financial level, both interconnection products are therefore to a first order substitutive. The decision between peering and transit reflects network planning considerations as well as direct cost considerations.[27] Transit incurs transport costs, but reduces the need to invest in the provider's own network. Peering requires the direct interconnection of the networks of both partners. This is relatively simple if the networks are spatially adjacent. Over longer distances, higher transport costs also arise for peering, e.g. due to the maintenance of an own Europe-wide backbone.

The cost function of Figure 1-13 shows a strongly degressive course (for each peering partner). This is explained by the fact that all relevant cost elements such as access, hardware, and premises are fixed costs. More precisely, they are fixed in relation to the capacity of the interface. The costs per Mbps therefore fall sharply with the amount of data exchanged.

Paid peering increases the unit cost for the paying company for any given volume of data. The curve shown in Figure 1-14 therefore shifts outwards and consequently the relevant intersection point also shifts outwards. Therefore, a higher volume of traffic is necessary for the transition from transit to paid peering to be warranted from the perspective of the paid peering partner.

Figure 1-14: Peering vs. Transit vs. Paid Peering



Source: WEKO (2014).

27 See BEREC (2012), p. 23.

A direct network connection via peering generally results in better quality for an end-to-end connection than an indirect connection via transit. With transit, the number of AS hops is at least 1 greater than with peering, with the result that the route becomes less attractive for the transit customer. The BGP path selection algorithm automatically gives preference to other available paths, which reduces the transported volume. Moreover, packet delays (latency and jitter) occur and response times increase. Furthermore, there is a greater probability of packet loss, because with the greater number of networks that have to be traversed, there is a greater probability of traffic congestion situations that can lead to the discarding of data packets. This applies in the upstream direction, but even more so in the downstream direction, because the response usually consists of a greater traffic volume than the request.

The study by Ahmed et al (2017) quantitatively estimated the quality differences of transit and peering. For this purpose, they carried out extensive quality measurements as application layer latency measurements for 510,000 customers in 900 ISP networks and multi-homed CDN servers in 33 IXPs worldwide. In general, peering paths had a higher quality than transit paths. Peering paths had lower delays for more than 95% of the ASes. This is the direct result of the shorter path lengths. Furthermore, peering paths had lower queuing delays in more than 50% of the ASes.

Furthermore, the authors found that peering paths result in a 5% improvement in end-to-end latency compared to transit paths for more than 91% of the ASes. In contrast, they determined a 5% improvement in latency for transit paths for only 2% of the ASes. Peering paths showed an improvement in delay of at least 5% for 95% of the ASes. Peering paths have at least 5% less queuing delay than transit paths for 57% of the ASes.

It is typical for Tier 2 ISPs to have both peering and transit relationships with other ISPs. Peering is used to reduce average costs and increase interconnection quality. Transit increases access to all regions of the Internet. Against this background, peering and transit are to a certain extent substitutes for each other. But they are not perfect substitutes and are not interchangeable for certain connections. In any case, peering and transit are complementary to each other.

Transit can also be seen as an alternative solution for interconnectivity if the (economic and contractual) prerequisites for peering are not met. By its very nature, such a back-up is also a temporary substitute in the event of a fault (failure of peering), provided that capacities permit.

Whether peering and transit are substitutable interconnection products cannot be decided in general, but only in individual cases. The question of substitutability depends on the customer and network structure of the interconnection partner. In any case, the following applies: The competitive relationships in peering and transit are interwoven. A peering (sub)market functions as a competitive market if and as long as ISPs can choose between different transit providers, and thus the transit (sub)market is competitive. In general, a peering connection is only a partial substitute for a transit connection with regard to the accessibility criterion, as peering only ensures connectivity between two specific network providers (and their customers) and not connectivity to the entire Internet. A complete substitution of transit by peering can therefore only be achieved by moving up to a tier-1 provider, which involves extensive investment and a substantial expenditure of time. In contrast, with regard to the quality of the connection to a particular network provider, peering can be seen as a substitute for transit rather than vice versa, as transit usually cannot reach the quality level of direct interconnection (peering).

1.3 Traffic via IXP

The BEREC 2017 Report notes with regard to Internet exchange points (IXPs) that multilateral peering, i.e. peering with more than two parties (as is the case with an IXP) was already the more prevalent approach compared to bilateral peering in 2011. In 2017, it was consequently expected that the use of IXPs would become even more important in the coming years as developing countries caught up with this trend. The report also noted that the volume of traffic exchanged through Europe's largest Internet Exchange Points (IXPs) in London, Amsterdam and Frankfurt was steadily increasing. BEREC's conclusion was that the non-profit IXP model is an efficient means of IP interconnection.

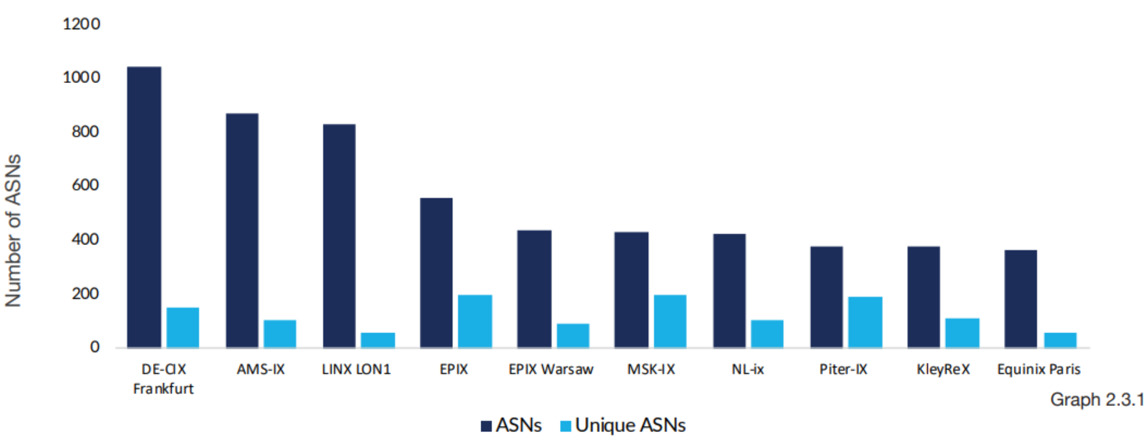
The developments of the past five years have not fully confirmed and supported the assessments and expectations of the relative importance of public peering via IXPs at that time. It is true that the traffic exchanged at IXPs has continued to grow as expected. But there are indications that traffic exchanged via bilateral private peering has increased relative to that exchanged via multilateral peering at IXPs. To that extent, the relative importance of IXPs for traffic exchange has decreased. This is also the conclusion of the ACM in its market analysis of 2021.[28] It is also clear from the example of DE-CIX in Frankfurt that the volume of traffic has not grown with the overall market. While more than 50% of IP traffic in Germany was handled there more than ten years ago, DE-CIX estimates that it is now (only) 25% or less.

The first thing to note is that the number of IXPs in operation in Europe has increased by 87.5% over the last 10 years, from 136 in 2010, to 255 in 2020.[29]

28 ACM (2021), p. 19f.
29 Euro-IX (2020), p. 6.

With regard to the total number of listed Autonomous System Numbers (ASNs) and the number of unique ASNs[30] in the Euro IX region at the end of 2020, Figure 1-15 provides an overview. It can be seen that DE-CIX Frankfurt leads the top ten with 1043 ASNs, followed by AMS-IX with 870 ASNs. The data also shows that the IXP with the most unique ASNs is EPIX, based in Poland, followed by MSK-IX and Piter-IX, both based in Russia.

Figure 1-15: Number of connected networks per European IXP, 2020



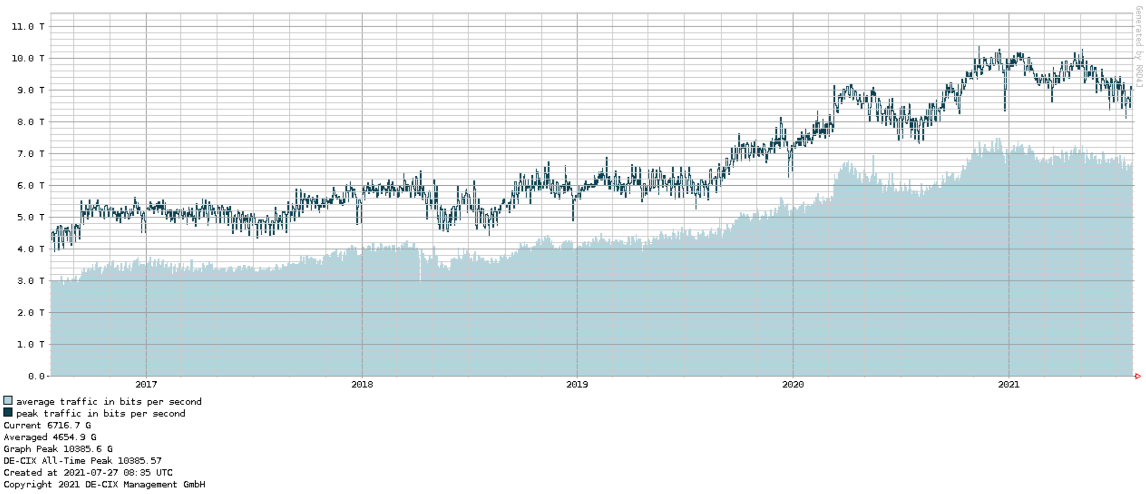
Source: Euro-IX (2020, p. 7).

By way of example, we show below the development of traffic volumes at the two Internet hubs of Frankfurt and Amsterdam, which are important for Europe.

Figure 1-16 shows the development of average data traffic and data traffic at peak times at the Frankfurt internet hub (DE-CIX) in the years from 2017 to 2021. The graph shows that this volume has increased significantly, especially since 2019. This corresponds to an average annual growth of 29%.

30 These are ASNs that are only connected to a specific IXP in the entire Euro IX region.

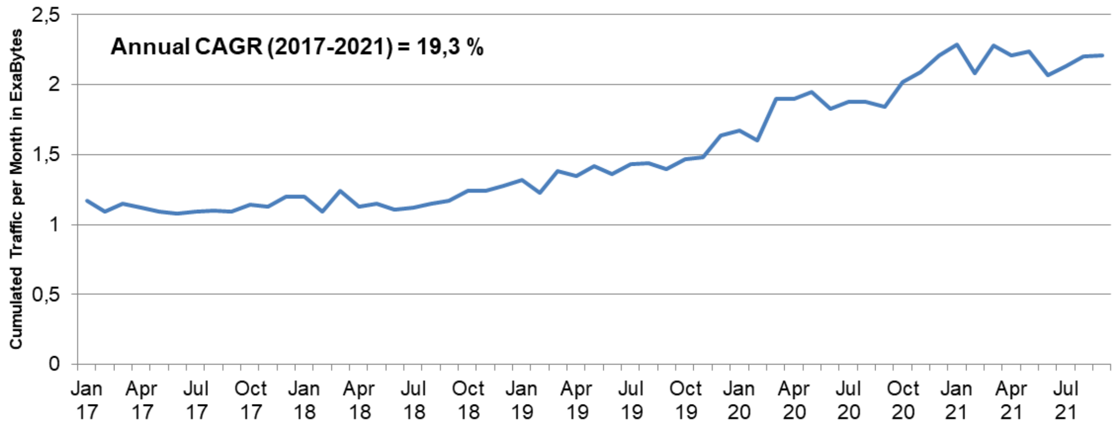
Figure 1-16: DE-CIX Frankfurt traffic in the years 2017 to 2021 (in Tbps)



Source: DE-CIX (2021).

Figure 1-17 shows the cumulative traffic of the AMS-IX Amsterdam site, the largest non-commercial internet node by traffic in the world. Traffic at this site has grown by 19,3% annually between 2017 and 2021 (CAGR), which is similar to Cisco's global IP traffic calculations for Central Europe between the years 2017 to 2022 (annual CAGR of about 22%, see Figure 1.1).

Figure 1-17: AMS-IX Amsterdam cumulative traffic (per month in exabytes)

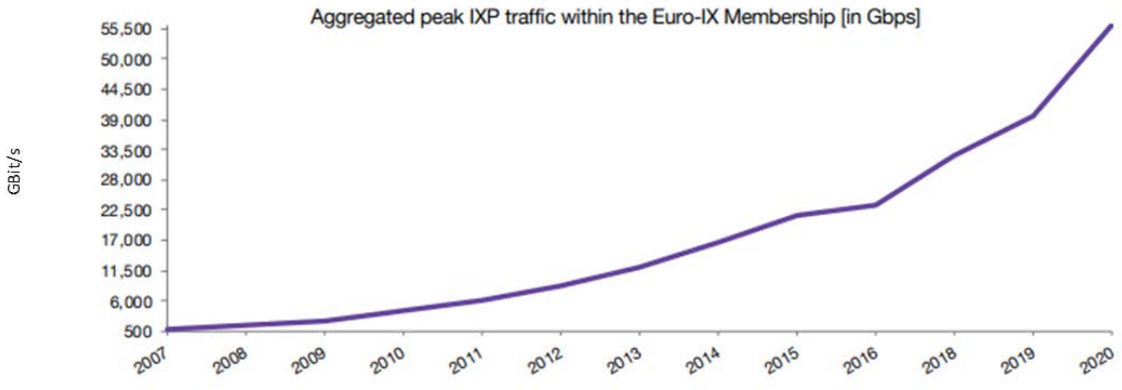


Source: AMS-IX (2021), values for annual CAGR are from September 2017 and 2021.

The data for all Euro-IX members also shows below-average growth compared to the total IP traffic. The aggregated peak traffic of the Euro-IX members grew by only 21.93% annually (CAGR) between 2017 and 2020. In the period from 2010 to 2020, the average growth rate was still at 27.15%.[31]

The vast majority of IRG members whom we interviewed reported that in their country, the incumbent telco is represented at one (or more) IXPs. We do not know with what capacity and with whom they exchange traffic there.

Figure 1-18: Traffic growth over ten years for Euro IX members



Note: The average number of IXPs from which data was collected was 56. This includes Euro-IX members and "sub-members", i.e. other IXPs or PoPs operated by their members in Europe, such as LINX Manchester, Netnod Gothenburg, etc. The aggregated peak traffic volume is calculated by collecting publicly available traffic statistics from Euro-IX. Member IXPs. The data was collected in 12-month periods from January to December each year and varied from one month to another depending on the available data (Euro-IX (2020, p. 10).

Source: Euro-IX (2020), p. 10.

In France, public peering traffic has traditionally had a relatively low profile compared to private peering and transit. Despite strong absolute growth, the relative share of public peering continued to decline there in 2020 to a share of only 2.9% (down from 3.1% in 2019).[32]

It remains to be seen whether public peering will continue to be of central importance for the functioning of the internet. However, it is clear that the relevant market players attach different importance to it for their own traffic exchange. Carriers of large volumes of traffic tend to turn away from public peering. For example, Deutsche Telekom was traditionally never connected to DE-CIX in Frankfurt. It is now connected there with a relatively low capacity of 20 Gbps, but implements a restrictive peering policy.[33]

31 Euro-IX (2020), p. 10.
32 ARCEP (2021), p. 41.
33 PeeringDB (2021a).

Private peering has a number of advantages for both large CAPs and large ISPs. Above a certain volume, it is not only cheaper than transit, but it also allows better monitoring of the quality of the traffic. The scaling of the interconnection with increasing end-user demand can be more evenly implemented.

The situation is different for smaller market players with lower data volumes. Public peering requires lower fixed costs of network interconnection for them than private peering. Public peering thus allows them to take advantage of the qualitative benefits of peering over transit with a lower data volume.

In recent years, however, IXPs have also been exposed to greater competitive pressure from data centre service providers. In addition to classic collocation, these offer their customers cost-effective options for bilateral interconnection via cross-connects, and thus substitute for services that are otherwise offered by IXPs. If several potential interconnection partners are already collocated at a data centre, it is relatively easy for the data centre operator to offer this customer an additional cross-connect at the same location. This business model combines the advantages of many-to-many interconnection at one location with the advantages of bilateral interconnection.

As more potential interconnection partners leave IXPs, the role and relative market strength of data centres is more likely to increase. Both ACM[34] and ARCEP[35] report the new role of data centres as interconnection providers for IP traffic, in direct competition with IXPs, in their recent market analyses. ACM expects an even stronger role for data centres in the long term. Compared to IXPs, they can leverage economies of scope between collocation and interconnection, together with pricing policy, and play them off against IXPs. ACM also reports fears in the market that the diversity of IXPs in the market could suffer, to the detriment of smaller market players.[36]

There are also indications in the literature that a decreasing relative importance of IXPs for traffic exchange follows from the endogenous dynamics of the internet itself. Böttger et al. (2019), for example, made two observations based on historical data from the public and voluntary peering database PeeringDB (which is used extensively in the ICT environment) in combination with routing paths. The emerging IXPs reduced the dependencies of ASes on Tier 1 providers and thus caused a "flattening" of the hierarchical structure of the Internet. In the process, the need for transit volumes was reduced and paths were shortened, which led to greater accessibility for smaller ASes, especially from so-called "hyper-giants". However, the tripling of IXPs and connected networks led only to an increase in reachable IP addresses to a level of 80%; since then, Böttger et al. find stagnation. Similarly, the authors find a movement of large, central ASes away from public peering at IXPs and towards private peering, while for smaller ASes, public peering plays a major role. From this, the authors conclude that

34 ACM (2021), pp. 25f.
35 ARCEP (2021), pp. 38f.
36 ACM (2021), p. 27.

the hierarchical nature of the internet, taking into account the relevance of public peering, is enduring. It should be noted that the analysis was carried out without taking traffic volumes into account.

1.4 Regionalisation of transport

In the IP Interconnection Study of 2012, BEREC stated and expected an increasing trend towards regionalisation of IP traffic.[37] The main reasons for this were the functioning of (local) CDNs and spatially distributed caching servers, a trend towards peering without the participation of Tier 1 backbone operators, and a high proportion of nationally produced content. BEREC furthermore reported an increasing trend towards originating traffic within a region. In 2017, BEREC reported an increasing share of interconnection among national networks.[38]

In the literature, there is a great deal of evidence confirming the trend of increasing regionalisation of transport. Doan et al. show this trend in the increasing market importance of CDNs.[39] Content caches are accessible within six IP hops. This can reduce IP path length by 40% for IPv4 and by 50% for IPv6. The more CDNs bring outsourced content to the (ISP) networks or to IXPs, the shorter the paths in the network and the greater the degree to which traffic remains regional.

The interviews also clearly substantiated this sustainable trend. A large ISP states that IP traffic is becoming more local. Transatlantic traffic and transit traffic have proportionately decreased significantly. The local/regional traffic transfer (from CDNs) is primarily driven by low-latency requirements. This is clearly illustrated by Netflix's CDN handover in Germany.[40] Netflix hands its traffic over to Deutsche Telekom's network at five regional locations. In total, Netflix operates its cache servers at 117 locations in Germany and can thus hand over traffic directly to regional and (large) local ISPs.

Deutsche Telekom's traffic structure also demonstrates the high concentration of traffic to a few customers on the one hand, and the strong regionalisation/localisation of traffic on the other. 70% of the traffic of the top 15 customers is transferred in Germany.

The investment behaviour of CAPs does not necessarily demonstrate a trend towards increasing regionalisation of transport. In a comparison between the periods 2011-2013 on the one hand and 2014-2017 on the other, Analysys found a +190% increase in CAPs' investments in North America, but only +68% in Europe.[41] Hosting accounts for the lion's share of these investments.

37 BEREC (2012), p. 35.
38 BEREC (2018), p. 39.
39 Doan et al. (2021), p. 2.
40 Open Connect Appliances (OCA) are Netflix's CDN (cache) servers, which can be integrated by ISPs into their networks to provide an on-net CDN.
41 Abecassis et al. (2018), p. 3.

1.5 CDN traffic

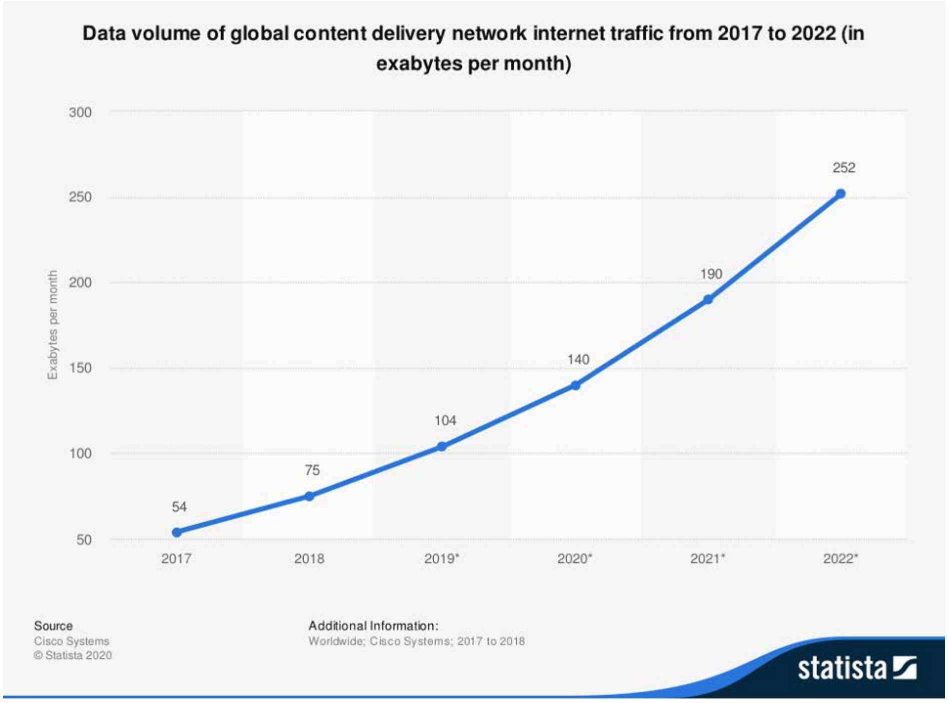
CAPs often use CDNs for the optimised distribution of their content, which shortens paths through the decentralised local storage of data. Here, Ahmed et al. (2017) distinguish between two common strategies: enter-deep and bring-home. The enter-deep strategy refers to the use of numerous smaller servers directly in the ISPs' networks, so-called on-net CDNs, which increases the global footprint and minimises the distances to their customers. Bring-Home refers to the approach of positioning servers at important strategic nodes such as IXPs or data centres with large capacities, where interconnection with many ISPs takes place via peering. As an example of the first strategy, Ahmed et al. refer to the Akamai CDN, which operates more than 325,000 servers in over 1,400 networks.[42] Limelight, on the other hand, operates servers in 135 locations and is connected to around 1,000 ISPs.[43] They also name Google and Netflix, whose strategy is a mix of both enter-deep and bring-home. These two options for local content provisioning via CDNs can result in different needs and dependence for peering contracts.

The economic importance of CDNs is steadily increasing. However, this does not apply to the classic commercial CDN business, but only to on-net CDN. In 2017, BEREC expected CDN traffic's share of total global internet traffic to increase from 45% in 2015 to 64% in 2020,[44] driven mainly by the increase in video streaming traffic. Proprietary CDNs are an economic option only for large CAPs. However, on-net CDNs or cache servers are becoming an increasingly common market reality. This is illustrated by data for France.[45] There, the share of on-net CDN traffic among the four largest ISPs has nearly doubled from 11% in 2016 to 21% in 2020. The wider use of on-net CDNs is also illustrated by the fact that the lower limit for requests for data stored on on-net CDN was between 8 and 25 in 2016, but only between 5 and 11 requests in 2020.[46] The particularly strong increase in CDN traffic in France in 2020 was primarily due to the change in usage behaviour during the COVID-19 pandemic.

Figure 1-19 shows the development of global CDN traffic since 2017. Traffic has almost tripled from 54 exabytes per month to 140 exabytes by 2020 and, according to this estimate, will almost double again by 2022. This would correspond to a CAGR of 18.9% in this overall period.

42 Akamai (2021a).
43 Limelight (2021).
44 BEREC (2017), p. 8.
45 ARCEP (2021), p. 44f.
46 The fact that data with a lower retrieval intensity is stored in CDN servers increases the overall use of on-net CDNs.

Figure 1-19: Global CDN Traffic 2017-2022



Source: Cisco Systems (2019) in Statista (2021).

According to Labovitz's (2019) analysis of internet traffic, 90% of residential internet traffic is delivered via CDNs. Ofcom estimated that 83% of fixed traffic was delivered by CDNs in 2017.[47]

Among the large CAPs, the share of traffic handled via CDN varies greatly. While Netflix delivers (almost) 100% of its traffic via its own CDN, Google delivers (only) a good 50%.

47 Ofcom (2017).

2 Developments in prices and costs

2.1 Cost trends

2.1.1 What are the relevant costs of peering?

In order to exchange peering traffic and operate interconnection, both interconnection partners must each provide one (or more) ports on a router on their side of the handover interface. These ports each have a capacity of 1 Gbps, 10 Gbps or 100 Gbps. Depending on the amount of traffic to be exchanged, several ports are used. If the capacity requirement is more than 1 Gbps, the use of one 10 Gbps port is typically more cost-effective than the use of two 1 Gbps ports. Similarly, one 100 Gbps port is more cost-effective than two 10 Gbps ports.

Regardless of the symmetry or asymmetry of the exchange of peering traffic, the capacity of the handover interface must be the same on both sides. Otherwise, direct interconnection on the link-layer protocol would not work technically. The interconnection costs of direct interconnection are the same for both peering partners.

The cost of a 10 Gbps port is on the order of a few thousand euros (~ 3,000 EUR). A 100 Gbps port does not cost ten times as much as a 10 Gbps port, but only about twice as much (as of 2020). The costs depend on the manufacturer's price and service model and on the quantity acquired.

In absolute terms, the costs of peering are therefore (approximately) the same or symmetrical for both peering partners. The costs of peering for each partner are fixed (or to be more precise, fixed step costs) that have a degressive course relative to the volume of data traffic exchanged. The cost of peering is primarily driven by the cost of routers and ports and any cost for the connection of both routers.

2.1.2 What are the relevant costs for transit?

Unlike with peering, the relevant costs of transit are not distributed symmetrically among the interconnection partners. The transit demand side initially incurs similar costs for the interconnection interface as with peering.

In addition to the costs of interconnection with the transit customer, however, the transit provider incurs additional costs. Depending on the traffic volume of the transit customer, the transit provider must present a larger interconnection capacity to its peering partners in order to carry the aggregate traffic of the transit customers. These additional costs can be attributed to the transit customers on the basis of cost causation. Furthermore, the transit provider incurs data transport costs in its own network for the transport of the transit traffic. Of course, only the portion of the data transport that required to reach end customers in other ISP networks is cost-relevant for the transit service, but not the portion of data transport needed to reach the transit provider's own end customers.

The data transport of the actual transit traffic through the transit provider’s network takes place from the data entry at one interconnection point to the exit at another interconnection point. These interconnection points can be located at a single site of the transit provider, or at two spatially separated sites. In the second case, traffic is routed through the transit provider's core network, to which all such interconnection points are connected. In cases where the transit connections are routed to national or international interconnection locations (e.g. IXPs), the capacity needed to carry the transit traffic to these locations is also relevant to the transit provider’s cost.

Thus, in contrast to peering, the costs for transit are determined by transport costs and costs for switches in addition to the costs for routers and ports.

2.1.3 The cost of the components

From international surveys of manufacturers and network operators, WIK has information about the price trends of network elements that are relevant for the technical implementation of peering and transit. The task of peering is realised by the Label Edge Router (LER), which serves as an interface to other networks, to CAPs, and to the provider's own network, and must therefore be provided at each peering location. This traffic is identified by the LER in the form of IP packets, provided with a so-called "label" and transferred to a Label Switch Router (LSR) for transport, which significantly reduces the delay of the transported traffic. In addition to transit traffic, these LSRs carry large volumes of the network's other traffic and are therefore not used exclusively for transit traffic. Thus, the LER is considered the decisive cost factor for peering, while the cost of the LSR is only partially relevant to transit.

LER and LSR each consist of interface cards (line cards) and housings for line cards (plug-in unit or PIU). PIUs and linecards must be dimensioned and matched to each other according to the transmission capacity requirement. The two network elements are therefore complements. Thus, the cost-determining characteristics of the individual PIU are the maximum traffic capacity, as well as the number of slots for line cards. The traffic capacity and the number of switchable ports (plus a reserve that network operators must keep in reserve) are likewise fundamental as regards the prices of line cards. Since a PIU is usually equipped with multiple line cards, line card price developments are of great relevance for network operators. Table 2-1 summarises the price trends observed over the past few years, and shows an overall downward trend in the price development of PIUs and line cards for both LER and LSR.

Table 2-1: Price development of the peering-relevant network elements LER and LSR[48]

		LER		LSR	
		2016-2018	2018-2020	2016-2018	2018-2020
	PIU	-8% bis -40%	-19%	-4% bis + 14%	-33%
LC	**10GE**	-55% bis -70%	-11%	-48% bis -71%	-37%
	100GE	-29% bis -34%	-11%	-20% bis -25%	-37%

Source: WIK Research.

A particularly significant price drop is visible for the 10GE (Gigabit Ethernet) interface cards of both network elements, LER and LSR. Thus, networks that have fewer economies of scale due to their size can also benefit from the general negative price trend. Purchase prices of the LER dropped by 55% to 70% over the period 2016-2018, depending on the number of ports, which corresponds to an annual rate of -18% to -23%. For the LSR, 10GE linecard prices reduced between 16% to 24% annually over the same period. Whereas the downward price trend in LER continues, but seems to be slowing down, we observe a continuation of the significant negative price trend in LSR.

In addition to the pure purchase prices for the relevant network elements, economies of scale also play a relevant role for network operators in terms of unit costs. If the traffic of the network increases, the cost allocation for the network element increases. The actual costs of large and small network operators can therefore develop differently. It should be noted that the handover between two networks is equally dimensioned, i.e. equal capacities must be kept available on both sides of the interconnection, and thus the costs in absolute terms of the peering between two networks are largely identical.

In the cost allocation of the LSR, which only partially fulfils transit tasks, the volume of other network data traffic is relevant for dimensioning and also for calculating unit costs.

In addition, the network elements of the Session Border Controller as a control and network routing device and the Domain Name Server have downstream cost relevance, although no price trend observations are available.

Transport in the backbone of the network, in which signals must be transported over long distances via optical fibres and wavelengths, i.e. also traffic that enters the network via peering and transit, is handled by multiplexer systems, so-called ROADM-OTN systems (Reconfigurable Optical Add-Drop Multiplexer/Optical Transport Network). For long distances, repeaters can be used to amplify the signal in the transmission between two points. Reliable price trend data for these transmission systems are available only for the period from 2018 to 2020, for which a partly significant price decline can also be observed.

48 Bandwidths result from price trends of different configurations of PIUs or line cards due to the query method.

Table 2-2: Price development for transmission systems

ROADM-OTN	
	2018-2020
PIU	-39%
Linecard	-58%
Repeater	-55%

Source: WIK Research.

While the prices for PIUs fell by an average of 13% per year between 2018 and 2020, the prices for line cards and repeaters fell by 19% and 18% respectively. This trend can also be observed in the aggregation network, in which DWDM systems are primarily used. There, the costs for PIUs fell by 24% and 27% for line cards in the same period. Overall, a declining price development for network operators can therefore also be seen for transport systems.

2.2 Pricing and billing principles for IP traffic

IP interconnection has traditionally been, and still is, done on the basis of transit and peering agreements and a bill-and-keep approach where the access provider/ISP does not receive payments at the wholesale level for terminating traffic. The access provider recovers its costs at the retail level by selling connectivity to the global internet to its end users. This billing model follows the “polluter pays” principle. Internet traffic is caused by end users; they retrieve data/information held and offered by CAPs. Peering and transit traffic occurs as a result of end users accessing the offer provided by CAPs. Peering partners usually handle this traffic among themselves free of charge according to the bill & keep principle. For supplementary paid peering and for transit, payment is made on the basis of the capacity provided at the POI. These costs are independent of where the traffic originates and terminates.

In contrast, voice traffic is billed according to the "Calling Party's Network Pays (CPNP)" principle. Pursuant to this billing principle, the network of the user initiating the traffic pays a termination charge at the wholesale level to the network operator of the called user. As the termination service is provided under a monopoly, it is typically regulated in order to prevent overpricing of the service.

There have been repeated calls from telcos to introduce the billing principle of end-to-end Sending Party Network Pays (SPNP) for the exchange of internet traffic and to levy traffic-dependent network charges (for the termination service) for internet traffic. In Europe, the last corresponding foray was undertaken by the telco incumbents organised in ETNO in 2012.[49] ETNO stated in its position paper in response to the relevant

49 ETNO (2012a).

BEREC consultation[50] that peering agreements are not free, as peering partners do not charge each other for traffic only if certain conditions are met. Therefore, traffic ratios in peering agreements are important because they reflect the costs of the parties involved. If there is a strong imbalance of traffic between two parties, there is no longer a solid basis for settlement-free peering. The consequence of continued settlement-free interconnection would be that the party sending a lower volume of traffic to the other network would have to bear negative effects in the form of higher costs than its counterpart. ETNO contends that settlement-free peering should therefore no longer be assumed in such a case.

BEREC opposed this approach in 2012[51] and advocated the unrestricted retention of traditional billing principles for IP interconnection. Although the importance of paid peering has increased significantly during the observation period of this study, according to the CAPs this should be the exception in Europe. Furthermore, we are not aware of any example of an ISP/incumbent telco in Europe introducing SPNP on its own.

Recently, there have been renewed initiatives to argue and advocate for the introduction of SPNP. The CEOs of 13 European telecom incumbents propose a new balance between the global technology giants and the digital ecosystem in Europe in a joint statement of 29.11.2021.[52] In the declaration, they specifically call for a "fair" participation of CAPs in network costs in order to (co-)finance further network investments (of ISPs).

The former head of the Austrian regulatory authority Georg Serentschy has also suggested the introduction of transit fees as a possible approach in this context.[53] Video streaming as a killer application and the COVID-19 pandemic would have increased the telcos' investment needs accordingly. Serentschy, however, places the discussion of transit fees in the context of a possible digital tax. In his view, a digital tax should be designed in such a way that it promotes investments in infrastructure. Transit fees represent, in his view, a possible form of implementation of a digital tax. For him, however, the question remains open as to how a kind of regulated transit fee for the telecommunications companies could be designed and what market failure would justify such a regulation.

South Korea is the only country so far to have introduced a billing mechanism that deviates from "Bill & Keep". In 2016, the SPNP billing principle was made mandatory by law for internet traffic between ISPs. Furthermore, in 2020 (large) CAPs were legally obliged to pay network fees to ISPs for terminating traffic on their networks. The legal

50 ETNO (2012b), p. 14.
51 BEREC (2012b).
52 ETNO (2021).
53 Serentschy (2021).

regulations in Korea, the subsequent interconnection disputes and the market implications are described in more detail in Section 2.1.1.

CAPs consider network charges payable to ISPs as rents for ISPs. CAPs put forward a number of arguments against the introduction of network charges for peering with ISPs.[54] For example, CAPs argue that ISPs have neither incentives nor obligations to use revenues from interconnection charges to expand network capacity or reduce end-user charges. They could also be used to buy content, for M&A activities, or simply for distributions to shareholders.

This argument is supported by Nikkhah and Jordan (2021), who have investigated the effect of paid peering fees on internet access prices and consumer surplus using a theoretical model. They derived welfare-theoretical implications for the dispute between ISPs and CAPs over network charges. ISPs argue that the imposition of network charges has no impact on their profits because peering charges are passed on to end customers in the form of low access prices. However, in their two-sided market model, Nikkhah and Jordan find that both positions are incorrect. With paid peering, prices for the premium price plan are reduced on the retail side, but increased for the basic plan. The shift in demand induced by this increases the ISP's profit. In this respect, not all of the revenue from peering is passed on to the end customers. Regarding consumer surplus, the authors find that it is a unimodal function of the paid peering fee. The fee that maximises consumer surplus depends on the price elasticities of demand for broadband access and video streaming. Under realistic assumptions about these elasticities, consumer surplus is maximised when paid peering fees are significantly lower than those that maximise ISP profits. However, this result does not mean that settlement-free peering maximises consumer surplus in all cases. The optimal peering price depends on the ISP's incremental cost per video streaming customer. Depending on the level of these costs, the price for direct peering can be negative, zero or positive.

Even though the results of this analysis depend on the parameterisation, the results provide important policy indications. Critically, it should be noted that a monopolistic ISP is used as a basis for the analysis, and thus the influence of competition between ISPs is not depicted. Transit as a possible substitute for (high) peering fees is also disregarded.

The collection of network charges could cet. par. be a double payment for the same traffic if end customers have already paid with their flat rates for the traffic they access at CAPs. However, charges can in principle also be collected from two sides, provided that overpayment is avoided. An important question is therefore whether the payment of network charges to ISPs from CAPs is intended to increase revenue or to redistribute it (retail charges may decrease and/or investments may increase).

---

54 For example, Netflix (2021), pp. 29ff.

Another argument put forward by CAPs is that the payment of network fees limits the possibilities for CAPs to invest in a (CDN) infrastructure that brings the content closer to the end customer.[55] This may also lead to additional costs for ISPs: If a CAP decides to route traffic over other networks where it does not pay network charges, this may mean that an ISP not only loses revenue from network charges, but may even have to pay (additional) transit charges.

Finally, CAPs argue that network charges would be an exploitation of the termination monopoly by ISPs for which there is de facto no market control. Depending on the CAPs' reaction to a charge, users could face restrictions in their choice of content or CAPs. This is especially true if CAPs are not able or willing to pay these fees.

In our assessment, competition between ISPs for end customers can set limits here, but this depends on the willingness of end customers to switch their ISP. It can be assumed that end customers switch CAPs more frequently than their ISP. Although CAPs can in principle avoid the obligation to pay network charges by seeking alternative routes to direct peering with an ISP, e.g. via transit, de facto these alternative options are - also in our estimation - limited. ISPs often control all routes into their network and determine capacity and price for all routes. When re-routing the content, for example, the transit capacities at the network junctions may not be sufficient to absorb the newly induced (large) volumes of traffic. The result would be congestion and a drastic drop in quality for the end customer. Thus, the way for ISPs to get a CAP to pay network charges would be to "congest" (i.e. leave undersized) all alternative routes (by transit ISPs) into the ISP's network. Such restrictive interconnection policies would result in poorer end-user quality for all CAPs not directly connected. Secondly, CAPs would be faced with the alternative of either paying network charges or accepting network congestion and quality degradation.

In our view, such an exploitation of the termination monopoly to levy network charges could also distort competition in the content market. In this context, many ISPs are in direct competition with CAPs for video streaming, either as cable network operators or as telcos with their own IPTV offering. Any degradation of competitors' TV/video offerings strengthens ISPs' own TV/video offerings. Creating bottlenecks (or failing to remedy them) at the network gateways therefore represents the greatest leverage for ISPs to enforce network charges. A further discussion of this issue in the context of the relative power structure between the various players can be found in chapter 5.1 of this study.

Furthermore, the literature documents a number of cases where this approach has been observed.[56] The developments in Korea as a result of the introduction of SPNP and of network charges for CAPs show that the possible effects mentioned above can actually be observed in the market.

55 Netflix (2021a), p. 7.
56 Lyons (2018), pp. 240ff.

2.2.1 Excursus: Case Study South Korea

In 2016, the obligation to use the Sending Party Network Pays (SPNP) settlement principle for IP transit was introduced in South Korea on the basis of a legal regulation. The law obliged the three Korean Tier 1 ISPs to settle transit charges among themselves according to the SPNP principle. Previously, ISPs had exchanged traffic among themselves settlement-free. In contrast to other parts of Asia, South Korea does not show a trend of falling transit prices. According to Telegeography, in 2021 transit prices in Seoul were 8.3 times higher than in Paris and 4.8 times higher than in New York. [57]

As a result, ISPs also charged network fees to CAPs. Some Korean CAPs then reduced the quality of their video services to save on network charges. Korea Telecom (KT) tried to pass on SPNP costs to Facebook as well. Facebook responded by shutting down its cache servers on KT's network and establishing the original traffic route. This slowed down access to Facebook for end-users of other ISPs who were previously served through these cache servers. SK Broadband (SKB), another major ISP, attempted to collect network fees from Netflix in 2019. When Netflix refused to pay, SKB appealed to the government to intervene, which the government refused to do. In November 2019, SKB applied for a decision from the Korea Communications Commission (KCC) to force Netflix to negotiate network fees.[58]

After the regulatory authority lost a legal dispute against Facebook on the question of whether services of a cache server can also be used beyond ISP network boundaries, the legislator made another legal change on the matter in May 2020. As part of an amendment to the Korean Telecommunications Act, CAPs were obliged to take "service stabilisation measures". In essence, large domestic and foreign CAPs were obliged to pay network fees to the ISPs. CAPs are obliged to do so if they have an average daily number of users of more than 1 million or if their traffic accounts for more than 1% of the total traffic in Korea. Furthermore, CAPs were made responsible for providing reliable access to their content. Unlike in South Korea, in the rest of the world this obligation applies to ISPs. This change in the law was also hotly contested. Open Net Korea and a number of other associations saw it not only as a violation of established principles of traffic exchange on the internet, but also as a violation of the principle of "Freedom of Speech", since a speaker would now have to pay for the distribution of his speech.[59]

The dispute over network charges is now also being fought out in court. In April 2020, Netflix sought a court declaration that there would be no obligation to negotiate network fees and no obligation to pay network fees.[60] The Seoul District Court rejected both of

57 Miller (2021).
58 See Kwang et al. (2021), Chambers and Partners, 5 July 2021.
59 Open Net Korea (2020).
60 See Kwang et al. (2021), Chambers and Partners, 5 July 2021.

Netflix's applications on 25 June 2021. Although the court found that Netflix had an obligation to pay, the court explicitly referred the parties to private autonomous negotiations (obligation) in the determination of the fee itself.

After Netflix continued to refuse to negotiate network fees, SKB filed a lawsuit in the District Court to explicitly require Netflix to pay network fees.[61] SKB demanded a payment of USD 22.9 million from Netflix for 2020.

In addition to Netflix, Google also refuses to pay network fees. In contrast, Amazon, Apple and Facebook now pay network fees to SKB.

Critics of the new internet policy development, such as Park and Nelson[62], point out that it will (further) weaken competition between ISPs in Korea and increase the cost of connectivity for all users in Korea. CAPs are already withdrawing from the Korean market, and the quality of their services is deteriorating. Korean CAPs are also particularly affected. They could not bear the higher costs of hosting their content in Korea. They either migrate out of the country, or are forced out of the market by large foreign CAPs. As a result of this change, Park and Nelson expect a decline in investment in network infrastructure and a slowdown in digital transformation in Korea. There is a conjecture that new submarine cable projects such as Google's Apricot, Facebook's Echo as well as Bitfrost will no longer land in Korea for these reasons.[63]

As a result of these implications, the legal regulation in Korea is under heavy pressure. Open Net Korea and 13 other NGOs see this as a violation of net neutrality.[64] They are calling on the responsible minister to revise the law and in particular to abolish the SPNP rule. They also highlight a loss of content diversity in Korea, as small and medium-sized CAPs in Korea would withdraw abroad to avoid paying network fees at home, and customers would eventually resort to foreign CAPs.

Abecassis and Kende argue and infer that the introduction of network charges through the SPNP billing principle will result in higher costs and more latency for Korean end-users when consuming content and services.[65] National CAPs typically host their content in Korea and previously only had to pay their ISP for connectivity. Now that these ISPs have to make payments to other ISPs for the delivery of the CAPs' content, these fees could be passed on to the CAPs. This would increase their costs compared to CAPs hosting in non-regulated markets. Abecassis and Kende therefore suspect that national CAPs may decide to make their content accessible from outside the country. This could further weaken their market position.

61 Lee (2021).
62 Park & Nelson (2021).
63 Google (2021a), Facebook (2021).
64 Open Net Korea (2020).
65 Abecassis & Kende (2020).

The second statutory regulation of 2020 already seemed to have been an initial reaction to these market developments. A size threshold clarified that only medium-sized and larger CAPs are obliged to pay these network fees.

The large international CAPs, on the other hand, have more options. They could interconnect directly with any ISP in Korea, thus avoiding (transit) payments between ISPs. They could also make content available to Korea outside Korea, where Korean ISPs would have to pick it up.

In fact, some CAPs have chosen to exchange traffic for Korea only outside Korea (in Asia or the US). This has increased both transit costs for ISPs and the risk of poorer quality of service.

2.3 Price trends for transit

Payment for transit is usually based on the peak capacity demanded, measured in Mbps. Usually, the higher bandwidth of both traffic directions determines the price for the transit service. Increasingly, billing is also done as a "metered" wholesale service without taking the traffic direction into account. Often, metering is done on the basis of the 95th percentile to determine the volume of traffic to be paid for. Here, the traffic is measured in 5-minute intervals. At the end of the billing period (typically one month), the measurement results are sorted, the top 5% of traffic is ignored and the 95% percentile is used.

In its 2017 study, BEREC identified a steady trend towards lower transit prices. In 2015, transit prices fell by as much as 33%.[66] In the period 1998 to 2012, transit prices had even fallen by 36% on an annual average. The absolute price for transit in 2015 was USD 0.63 per Mbps.

Falling prices were and are driven by technological progress and competition in the transit market. Transit continues to come under increasing pressure from peering and CDN services. The trend towards falling transit prices has continued, albeit at a slower pace.

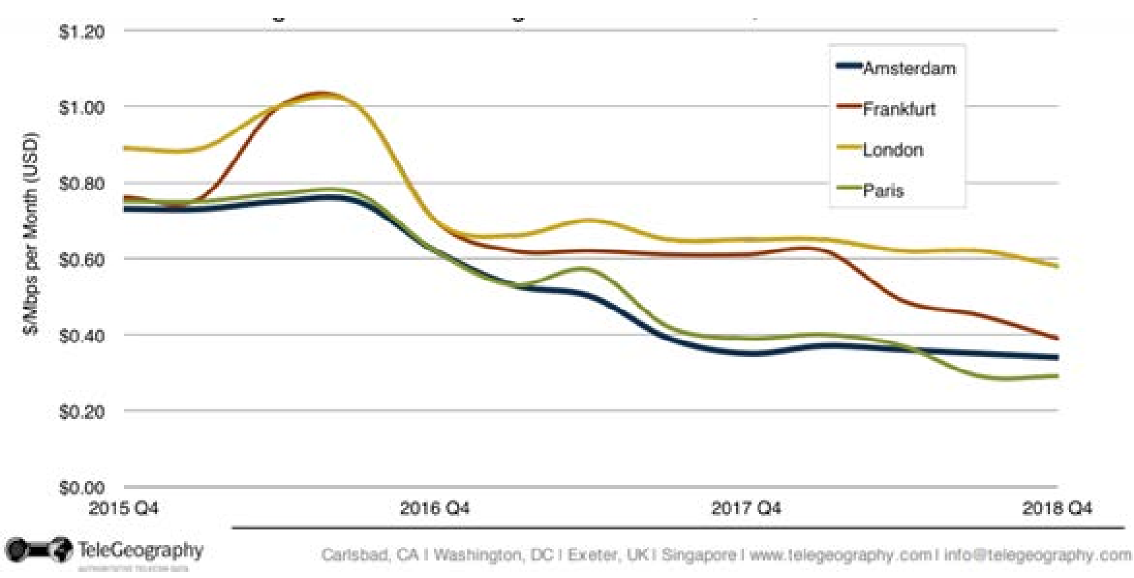
Many market participants assume that the price trend for transit is driven by technological progress, which allows equipment with higher bandwidth to be provided at lower cost.

66 See BEREC (2017), p. 8.

In a sample of markets, 10 GigE (Gigabit Ethernet) prices fell 18% annually between the second quarter of 2018 and the second quarter of 2021. In a comparable survey of 100 GigE port prices, prices fell by 30% over the same period.[67]

According to a study by TeleGeography, recent price declines have been strongest in emerging markets where previous prices were comparatively high, particularly in Latin America. Similarly, prices continue to fall in the established global hubs.[68]

Figure 2-1: Weighted Median 10 GigE IP Transit Prices in Europe, 2015-2018



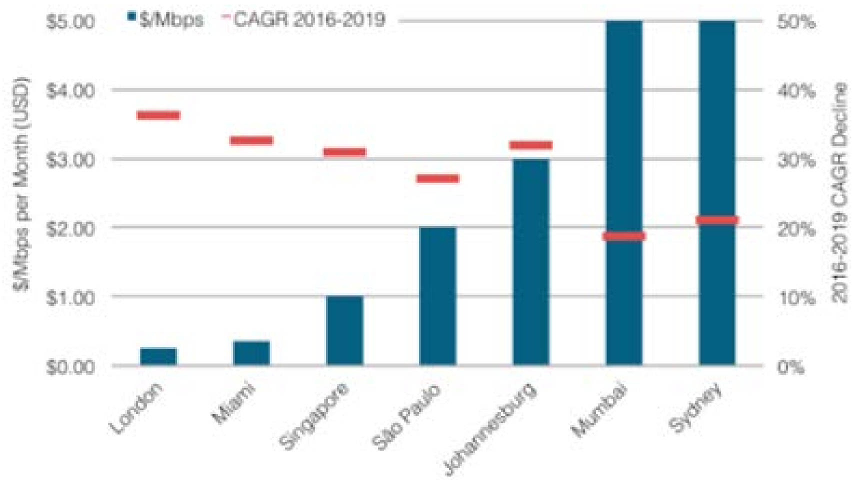
Source: Hjembo (2019), p. 45.

For the Frankfurt location, an annual price decline (CAGR) of approx. 18% can be observed between 2015 and 2021 (weighted median 10 GigE IP transit price).[69]

The IP transit price has fallen by 20-40% annually in the main hubs between 2016 and 2019 (see Figure 2-2), and by about 20% over the period 2018-2021 (see Figure 2-3). Singapore, Miami, London are depicted in both time periods. These locations have thus seen a reduction in price declines over the last three years compared to the 2016-2019 time period.

67 Coll (2021b).
68 Coll (2021b).
69 Own calculations based on Hjembo (2019) and Reilly (2019).

Figure 2-2: Weighted median 10 GigE IP transit prices and three-year CAGR decline in major global locations, Q2 2019 (2016-2019).



Notes: Each column represents the weighted median monthly price per Mbps in the listed city. The line represents the percentage decline of the weighted median price calculated as a three-year compound annual growth rate. Prices are in USD and exclude local access and installation fees. 10 Gigabit Ethernet (10 GigE) = 10,000 Mbps.

Source: Reilly (2019).

Figure 2-3: Weighted median 10 GigE and 100 GigE IP transit prices and 2018-2021 CAGR decline in key global locations.

Source: Coll (2021b).

Furthermore, it should be emphasised that the publicly available transit prices represent average values. The individually and bilaterally negotiated prices show a considerable dispersion. For example, ARCEP reports that negotiated individual prices in France ranged from less than €0.1 to several euros per Mbps per month.[70] ACM highlights that smaller market players benefited less from price reductions than the larger ones.[71] They pay a relatively higher price for their lower bandwidth. This follows both from higher transit prices themselves and from lower economies of scale. For example, a 100 GE/Gbps interface is only about 10 times as expensive as a 1 GE/Gbps interface.

Deutsche Telekom reports a transit price level of about 10 cents. Large CAPs pay even less than 5 cents. Deutsche Telekom tries to counteract the trend of falling prices, but in any case not to allow prices to fall faster than the simultaneous increase in traffic can compensate for. This is an attempt to keep the revenue from transit more or less constant. Strategically, they achieve this by positioning their transit product as a premium product. Despite following the principle of non-discrimination in prices, these vary to a significant degree. The pricing models also include discounts based on contract length, traffic volumes, purchase obligations and the number of exchange points. Deutsche Telekom's average price for transit is currently 20 cents.

It can thus be said that the trend of falling transit prices has continued as expected. Transit in Europe now costs less than a third of the price in 2015, but the rate of reduction has slowed.

2.4 Peering price trends

2.4.1 Peering Policies

Peering agreements are usually concluded on the basis of an ISP's or CAP's peering policy laid down in a publicly accessible or confidential document. The peering policy describes the terms and conditions under which the respective market player offers peering. The exact peering policies are only publicly known in a few cases.

Peering policies can be open and uniform or selective. Furthermore, peering policies can be more or less restrictive. They can set up high or low barriers for this form of interconnection. There are also (relevant) players that do not have a (uniform) peering policy or do not offer peering at all. In any case, a peering policy defines a unilateral act.

Typical conditions under which market players enter into peering are:

- Strict traffic exchange between two ASes;

70 ARCEP (2021), p. 45.
71 ACM (2021), p. 16.

- Implementation of dedicated bandwidth for traffic exchange;
- Minimum volume of traffic to be exchanged or minimum capacity of the interconnection interface;
- Requirements for the size of the partner's international backbone;
- Number of traffic exchange points;
- Routing preferences;
- Requirements for the ratio between inbound and outbound traffic;
- Prohibition of simultaneous transit.

In some cases, ISPs require a certain ratio of inbound and outbound traffic for settlement-free peering and require paid peering where there is a deviation. In many cases, changes to unilateral peering policies in existing peering relationships are contentious.[72]

In its 2021 market analysis, ACM describes the peering policies of the main ISPs in the Netherlands. These are shown in Table 2-3 and Table 2-4. According to this information, the smaller ISPs tend to have a more open peering policy than the larger ones. Compared to 2015, the peering policy has become more restrictive. Although ACM understands the business logic of large players peering only with large partners, this creates barriers to entry for new (or small) CAPs, CDNs, small ISPs and hosting providers until they are large enough to deliver comparable traffic volumes. These disadvantages for smaller CAPs and CDNs also depend on the type of content they provide.

Table 2-3: Peering policies of the largest ISPs in the Netherlands

Company	Multiple locations	Ratio requirement	Contract requirement
KPN	Desired	Yes	Yes
GTT (formerly KPN International)	Required - international	Yes	No
VodafoneZiggo	Not required	No	No
VodafoneZiggo	Preferably	Yes	Yes
Liberty Global [73]	Required - international	Yes	Yes
T-Mobile	Required - EU	Yes	Yes
T-Mobile	Not required	Yes	No
Deutsche Telekom	Required - international	Yes	Yes
Delta Fiber Nederland (Zeelandnet)	Desired	No	Private only
Delta Fiber Netherlands (CAIW)	Preferably	No	Private only

Source: ACM (2021), p. 15.

72 See for example the interconnection dispute between Init7 and Swisscom in 5.2.1.1.
73 Gallimore (2021a).

Table 2-4: Peering details of the largest ISPs in the Netherlands

Company	Network number	Number of *peering* locations in the Netherlands	Locations: local, regional, global	*Traffic level*	*Public peering* where?
KPN	AS1136	6 (*public peering*)	regional	1-5 Tbps; mostly *inbound*	*Peering* via NL-IX and R-IX only
GTT (formerly KPN International)	AS286	3 (*public peering*) 10 (*private peering*)	global	1-5 Tbps; mostly *inbound*	*Peering* through AMS-IX NL-IX, R-IX,
VodafoneZiggo	AS33915 AS9143	2 (*public peering*) 9 (*private peering*)	Europe regional	50-100 Gbps, mostly *inbound* 5 Tbps; mostly *inbound*	*Peering* via AMS-IX
Liberty Global [74]	AS6830	5 (*public peering*) 4 (*private peering*)	global regional	7 Gbps *balanced* (1:3) traffic	*Peering* via AMS-IX, NL-IX, Asteroid, Equinix
T-Mobile	AS31615 AS50266	0 (*public peering*) 1 (*private peering*) 4 (*public peering*) 2 (*private peering*)	regional regional	-, mostly *inbound* -, mostly *inbound*	- *Peering* via AMS-IX, NL-ix
Deutsche Telekom	AS3320	1 (*public peering*) 3 (*private peering*)	global	50-100 Tbps Mostly *inbound*	*Peering* via AMS-IX
Delta Fiber Netherlands	AS15542 (Zeelandnet)	0 (*public peering*) 6 (*private peering*)	regional	100-200 Gbps, Mostly *inbound*	-
Delta Fiber Netherlands	AS15435 (CAIW)	4 (*public peering*) 2 (*private peering*)	Europe	300-500 Gbps, Mostly *inbound*	*Peering* via AMS-IX, NL-ix

Source: ACM (2021), p. 15.

Deutsche Telekom implements a comparatively restrictive peering policy. They fundamentally offer peering only to Tier 1 operators. This policy dates back to the beginnings of the expansion of the Internet and has been (consistently) maintained ever since. In 2001, Deutsche Telekom had built up a worldwide international backbone in order to achieve the status of a Tier 1 provider. Deutsche Telekom's peering agreements contain a strict traffic ratio for ingoing and outgoing traffic. As soon as the ratio of 1:1.8 is exceeded, settlement-free peering turns into commercial transit and payouts occur in one direction or the other.

The consequence of this peering policy is that all CAPs do not have a peering relationship with Deutsche Telekom, but a (technical and commercial) transit relationship. Technically, they have access to Deutsche Telekom's entire routing matrix at the network gateways (regardless of whether they need or demand this). Commercially, the CAPs pay transit fees to Deutsche Telekom. In fact, the large CAPs

74 Gallimore (2021b).

do not use the entire routing table that comes with DT's offer, but only serve the routes with which they reach the end customers in Deutsche Telekom's network. In this respect, the interconnection is technically operated by the CAPs as peering.

Deutsche Telekom likewise does not perrmit on-net peering for commercial CDNs or for in-house CDNs of the CAPs. The cache servers of CDNs are not installed in the Deutsche Telekom network. They are located beyond the network delivery points. The large CAPs maintain not just one but usually five transfer points to the Deutsche Telekom network (Frankfurt, Munich, Berlin, Hamburg and Düsseldorf). Deutsche Telekom does not currently see the need for further cache locations. Five locations are sufficient for the latency requirements throughout Germany. In the medium term, however, an expansion to further network transfer points is expected.

Deutsche Telekom justifies this peering policy by the need to ensure quality for the end customer. Furthermore, Deutsche Telekom wants to maintain control over its own network and considers its transit offer to be a premium product.

The peering policy described also has an impact on Deutsche Telekom's presence at the public Internet node DE-CIX. Deutsche Telekom does not offer peering to potential interconnection partners here either, but only a service that both technically and commercially is transit. The presence at DE-CIX plays only a subordinate role for Deutsche Telekom's IP traffic exchange. Network interconnection only takes place here with a few small and specialised customers.

To survey the peering offers and peering policy for the German market of important ISPs and CAPs, we evaluated the PeeringDB database as of 01.11.2021. The PeeringDB contains information on the locations of public and private peerings as well as the peering policy. All information in the database is voluntary. However, according to many market players, the information in the database largely corresponds to the real situation. For Table 2-5 and Table 2-6 we have enriched the PeeringDB data with information from the IXP database and private peering points. The number of locations shown does not take into account the number of ports available.

Table 2-5: Peering details of large ISPs and CAPs in Germany

Company	ASN	Number of public in GER	Number priv. in GER	Geographical scope	Traffic volume	Traffic direction
Akamai Technologies	20940	8	10	Global	100+Tbps	Strongly outgoing
Limelight Networks Global	22822	5	3	Global	1-5Tbps	Predominantly outbound
NetCologne	8422	3	3	Europe	500-1000Gbps	Predominantly inbound
Telefónica Germany	6805	7	6	Europe	1-5Tbps	Balanced
Deutsche Telekom	3320	1	14	Global	50-100Tbps	Predominantly inbound
IONOS	8560	2	2	Global	300-500Gbps	Predominantly outbound
Vodafone Germany	3209	5	7	Regional	n.a.	Predominantly inbound
EWETel	9145	5	2	Regional	200-300Gbps	Predominantly inbound
Netflix	2906	6	5	Global	n.a.	Strongly outbound
Lumen AS3356	3356	0	0	Global	100+Tbps	Balanced
1&1 Versatel Germany	8881	5	9	Europe	1-5Tbps	Predominantly inbound
Facebook	32934	11	7	Global	100+Tbps	Strongly outbound
Dailymotion	41690	1	0	Global	n.a.	Strongly outbound
Zattoo	8302	2	2	Europe	n.a.	Strongly outbound
STRATO	6724	2	2	Europe	n.a.	Predominantly outbound
M-net	8767	5	6	Regional	200-300Gbps	Predominantly inbound
Amazon.com	16509	4	6	Global	n.a.	Balanced
Hetzner Online	24940	3	9	Europe	5-10Tbps	Predominantly outbound
Amazon IVS / Twitch	46489	3	7	Global	n.a.	Strongly outbound
Tele Columbus	20880	2	0	Regional	50-100Gbps	Strongly inbound
Deutsche Glasfaser	60294	2	5	Europe	200-300Gbps	Predominantly inbound
Trivago	198018	1	0	Global	n.a.	n.a.
Zalando	201026	1	0	Europe	5-10Gbps	Predominantly inbound
rtl2television	206549	0	2	Europe	1-5Gbps	n.a.
Facebook AS63293	63293	1	0	Global	n.a.	Strongly outbound
Akamai Direct Connect	20189	0	2	n.a.	n.a.	n.a.
Sky Germany	208452	0	3	Europe	n.a.	Predominantly outbound

Source: WIK Research.

If one adds private and public peering locations, Akamai and Facebook, with 18 locations each, have even more peering locations than DT (14) in Germany. Both providers also show a larger traffic volume than DT with more than 100 Tbps. It is remarkable that regional ISPs with a relatively low traffic volume such as NetCologne (6), EWETel (7) and M-net (11) also have relatively many peering sites. It is also surprising that both Telefónica Deutschland and Amazon show balanced traffic despite the usually asymmetrical data consumption of end customers (more download than upload). This cannot be observed with other end-user ISPs, for example.

Table 2-6 shows essential features of the peering policy of the same ISPs and CAPs in the German market. While most peering providers prefer multiple handover points, only a few (such as DT, Limelight, Lumen, 1&1 Versatel) make this a requirement for peering. Only DT requires a certain ratio of inbound to outbound traffic for peering. Furthermore, only DT, Vodafone, Lumen and Akamai Direct Connect require an explicit contractual relationship. For all others, peering is based on a traditional "handshake arrangement".

Table 2-6: Peering policies of large ISPs and CAPs in Germany

Company	Multiple transfer points	Traffic ratio	Contract required
Akamai Technologies	Not required	No	Not required
Limelight Networks Global	Required - USA	No	Not required
NetCologne	Not required	No	Not required
Telefónica Germany	Preferred	No	Not required
Deutsche Telekom	Required - International	Yes	Required
IONOS	Preferred	No	n.a.
Vodafone Germany	Preferred	No	Required
EWETel	Preferred	No	Not required
Netflix	Not required	No	Not required
Lumen AS3356	Required - International	No	Required
1&1 Versatel Germany	Required - EU	No	Not required
Facebook	Not required	No	Not required
Dailymotion	Preferred	No	Not required
Zattoo	Not required	No	Not required
STRATO	Not required	No	Not required
M-net	Not required	No	Not required
Amazon.com	Preferred	No	Not required
Hetzner Online	Not required	No	Not required
Amazon IVS / Twitch	Preferred	No	Not required
Tele Columbus	Not required	No	Not required
Deutsche Glasfaser	Not required	No	Not required
Trivago	Not required	No	Not required
Zalando	Not required	No	Not required
rtl2television	Not required	No	Not required
Facebook AS63293	Not required	No	n.a.
Akamai Direct Connect	Preferred	No	Required
Sky Germany	Not required	No	Not required

Source: WIK Research.

2.4.2 Settlement-free vs. paid peering

The world's most comprehensive study to date on the network economics of the internet was prepared by Weller/Woodcock (2013) for the OECD's Internet Recommendations of 2013. The data basis of the study was updated for BEREC in 2016.[75] The data

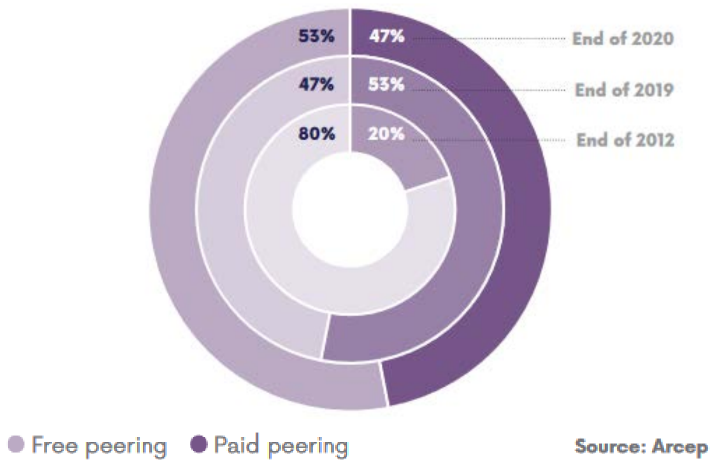
75 See Woodcock & Frigino (2016).

analysis in 2016 was based on 1,935,822 inter-carrier interconnection agreements. Only 0.07% of all agreements were formalised contracts. In 2011, this rate was still 0.49%. In 99.98% of the agreements the conditions were symmetrical. Both sides gave each other the same conditions. Only 403 agreements were based on asymmetrical conditions. Typical asymmetries were payments for routes that could not be reached otherwise and the requirement of minimum conditions for peering and paid peering.

BEREC suggested at the time that the traffic share of paid peering was much higher than reflected in the contract structures mentioned. For Europe in particular, paid peering was expected to be a common contractual practice of the major European ISPs. The transition from settlement-free to paid peering often followed interconnection disputes over the handling of rapidly growing and increasingly asymmetric traffic. However, the CAPs we interviewed unanimously report that settlement-free peering is still predominant in Europe. There are only a few exceptions to this general principle, each of which has its own individual history.

The trend towards ever greater volumes of traffic being handled via paid peering is reflected in the market data for France. Whereas in 2012 only 20% of peering traffic was exchanged via paid peering, in 2019 this figure had already risen to 53% (s. Figure 2-4).

Figure 2-4: Evolution of the share of Paid Peering at the main 4 ISPs in France



Source: ARCEP (2021), p. 44.

Remarkably, there was a trend reversal in 2020. The share of paid peering declined again to 47%. ARCEP cites two reasons for the trend reversal: Firstly, due to the increase in settlement-free peering between partners of comparable size and secondly, due to the substitution of paid peering traffic between CAPs and ISPs by on-net CDNs.

ACM (2021) sees the discussion on settlement-free and paid peering between the large ISPs and the large CAPs as relaxed by now. The relationship with each other has become more balanced, united in the interest of producing good quality for the end customer. The question of payment for peering, on the other hand, is becoming less important.

However, this increasing balance of interests between large ISPs and large CAPs does not apply to smaller market players. Economies of scale are very important. Market entry and expansion is therefore difficult for smaller players. Entering settlement-free peering therefore presents a high barrier for them. Peering and especially settlement-free peering is difficult to obtain for small ISPs and CDNs and is rather reserved for a more or less closed club of large market players.

2.4.3 Price trends for private peering

BEREC did not provide any data on paid peering prices in 2017. The non-transparency of these prices remains unchanged. ACM reports discussions with market players, according to which the prices for private peering vary widely, ranging from a few cents to a few tens of cents per Mbps per month.[76] Prices are determined by the expected added value of the interconnection for both parties and the degree of their market power. ARCEP still reports an even wider range of prices for private peering, from €0.25 to several euros per Mbps per month.[77]

ACM estimates the costs of private peering for an ISP to be relatively low. In any case, the costs for public peering (per unit) are higher. The costs of IP connectivity payable to third parties are also relatively low compared to the maintenance of the access and core network as well as for content procurement.

2.5 Price trends for CDNs

According to ARCEP's data, in most cases no fees are charged for on-net CDNs.[78] However, within the framework of larger paid peering agreements between CAPs and ISPs, payment for CDN services may also be made.

BEREC reported persistently falling CDN prices in 2017.[79] Prices fell by 20% in 2015 and by 25% in 2014. Prices themselves vary between operators and depend on the size of customers. BEREC observed and expected a similar price trend for CDNs as for transit in the future, as both prices are strongly driven by economies of scale and they influence each other.

76 ACM (2021), p. 17.
77 ARCEP (2021), p. 45.
78 ARCEP (2021), p. 45.
79 BEREC (2017), p. 34f.

2.6 Price trends for public peering

Prices for public peering typically consist of one-time fees for connection to the IXP and a monthly fee per port used (with a maximum capacity for data traffic per period of time). ACM has published a price comparison for major European Internet exchanges (as of January 2021) in its 2021 market study.[80] We have updated this price comparison with our own data collection. According to this, the prices for a 10 GE/Gbps port fluctuate around an average of 611€ and for a 100 GE/Gbps port of 3,035€. This results in an average price per Mbps (at 85% utilisation) of 3.57 cents for a 100 Gbps port and 7.18 cents for a 10 Gbps port. The 10 Gbps port price is below the benchmark average at ECIX, and the 100 Gbps price is slightly above it. Relatively high prices are charged in Paris.

Table 2-7: Peering Prices of Major European IXPs

Internet Exchange Points	**100 Gbit/s Port Price** in Euro	**10 Gbit/s Port Price** in Euro	**100 Gbit/s port:** Monthly Mbit/s price at **85% utilisation** in euro cents	**100 Gbit/s port:** Monthly Mbit/s price at **40% utilisation** in euro cents	**10 Gbit/s port:** Monthly Mbit/s price at **85% utilisation** in euro cents	**10 Gbit/s port:** Monthly Mbit/s price at **40% utilisation** in euro cents
AMS-IX (Amsterdam)	3600	720	4,20	9,00	8,50	18,00
LONAP (London)	1759	268	2,10	4,40	3,20	6,70
LINX LON1 (London)	3405	708	4,00	8,50	8,30	17,70
LINX LON2 (London)	2203	454	2,60	5,50	5,30	11,40
SwissIX (Zurich)	2388	430	2,80	6,00	5,10	10,80
BCIX (Berlin)	2628	514	3,10	6,60	6,00	12,90
ECIX (Germany)	3278	528	3,90	8,20	6,20	13,20
BNIX (Brussels)	2628	717	3,10	6,60	8,40	17,90
FranceIX (Paris)	4300	850	5,10	10,80	10,00	21,30
Equinix (Paris)	3861	792	4,50	9,70	9,30	19,80
NetNod (Copenhagen, Stockholm)	3340	742	3,90	8,40	8,70	18,60
Arithmetic mean of the prices	3035,45	611,18	3,57	7,61	7,18	15,30

Source: Sniders et al. (2021) on Peering.exposed, method according to ACM (2021), WIK Research.

80 ACM (2021), p. 17.

3 Market position of the market players

3.1 Cash flows and dependencies

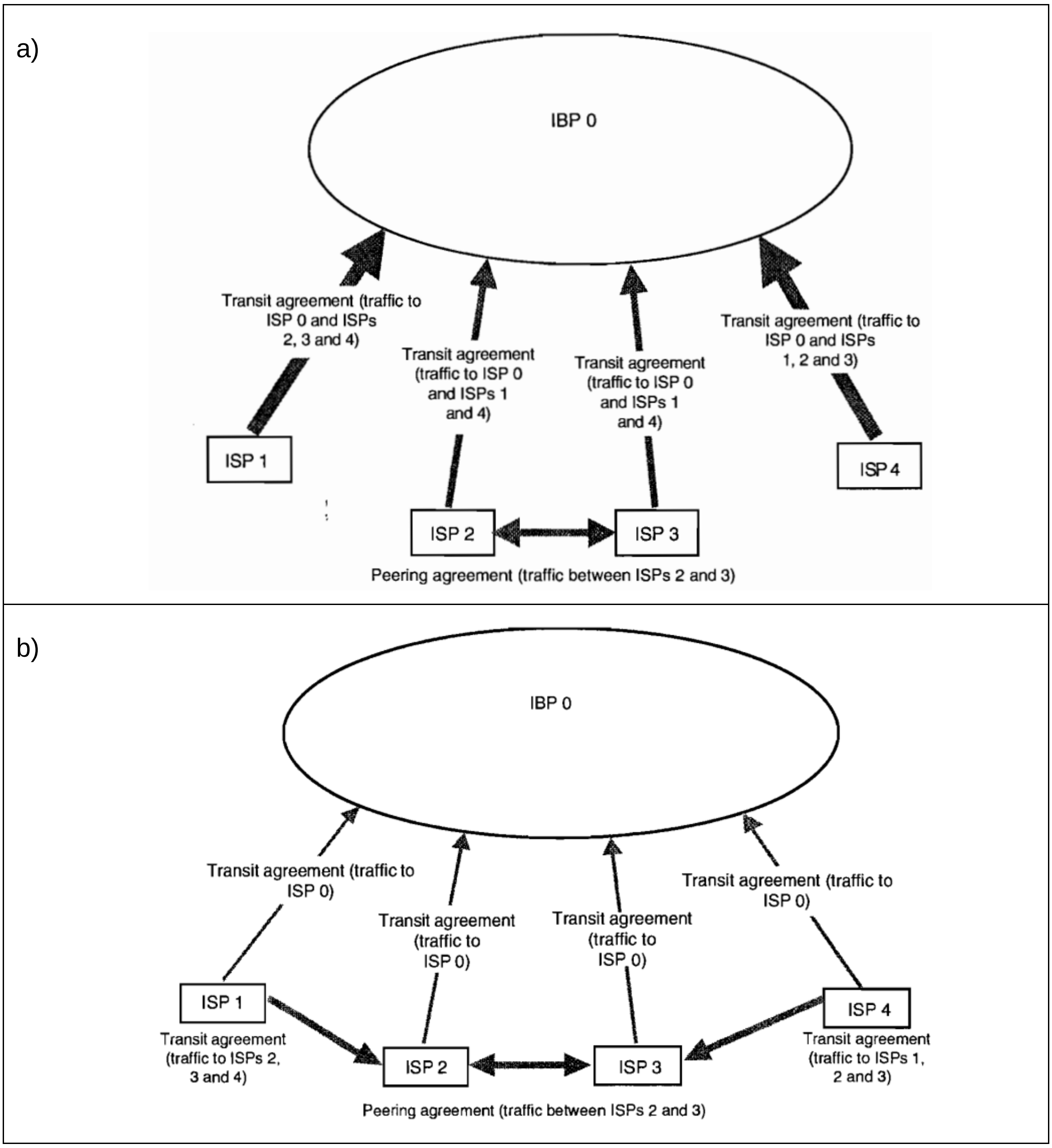
The payment flows in the area of internet interconnection usually flow from end-users and business customers primarily via end-user ISPs towards the downstream backbone ISPs in the value chain. End-users (eyeballs), or business customers, value access to the entire Internet and therefore purchase an Internet access service, which is usually differentiated by ISPs based on the dimensions of bandwidth and/or data volume and includes connectivity to the global Internet.

Thus, these revenues are (at least partially) passed on to downstream backbone ISPs in the form of transit fees. The volume of this expenditure depends directly on the extent of the total traffic volume of an ISP that can be handled via (settlement-free) private or public peering. Figure 3-1 a) and b) illustrate the expected changes in payment flows between an exemplary selection of ISPs if changes in transit costs (or transit connectivity) occur.

Figure 3-1 a) shows an example of a situation with 4 (end-user) ISPs and one backbone ISP, which supplies these ISPs with transit. While ISP 2 and ISP 3 peer directly with each other and therefore need to buy less transit from ISP 0, ISP 1 and ISP 4 are completely dependent on the transit service of the backbone ISP (ISP 0) to provide connectivity to their own customers.

If ISP 0 were to increase its prices for transit, the other market participants could react accordingly to the price increase. Figure 3-1 b) illustrates this case. In this situation, it can be assumed that ISP 2 and ISP 3 use the existing peering agreement among themselves to offer ISP 1 and ISP 4 (partial) transit as a service. Thus, in this case, the demand of the four ISPs for the service of the backbone ISP (ISP 0) is reduced to connectivity to its own customers. Whereas ISP 0 in this example provided the primary connectivity between the four ISPs before the price increase, its role after the price increase is reduced to only providing those routes that the four ISPs cannot serve themselves (regardless of the resulting payment flows among themselves, i.e. peering or transit). Of course, the relative size of these four ISPs in relation to the size of ISP 0 (e.g. number of customers served) determines whether these remaining routes are a substantial or merely a negligible part of the routes essential for the end and business customers of ISP 1-4.

Figure 3-1: Reaction of interconnection partners to a price increase or degradation of transit



Source: Economides, N. (2004). Fig. 3 (p. 396) & Fig. 4 (p. 397).

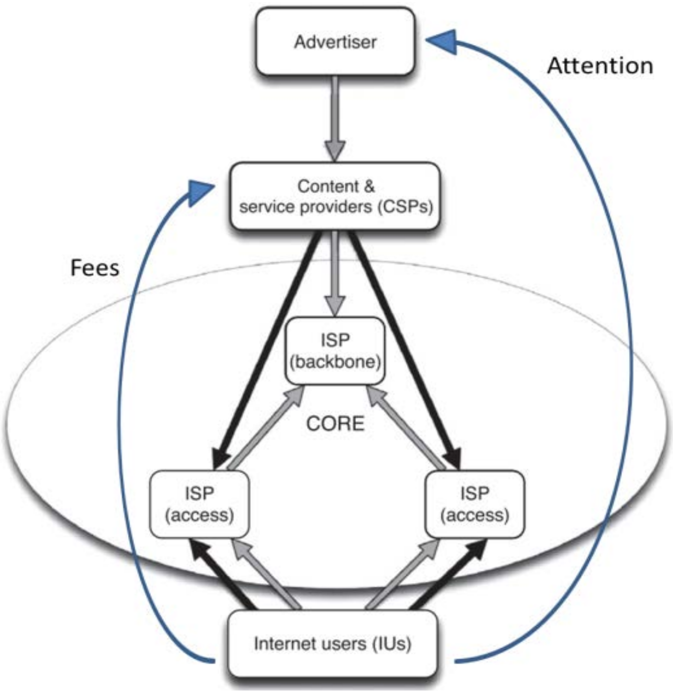
This example directly illustrates that price increases represent an opportunity for competitors and potential entrants. The increasingly meshed architecture or direct connectivity between players therefore makes corresponding strategies of players in the value chain increasingly unattractive.

However, CAPs and their paid and/or ad-financed content offers result in additional payment flows, which arise from the corresponding service fees or indirectly from the attention of consumers and flow past the ISPs (directly or indirectly) to CAPs. Although this value creation presupposes existing connectivity by ISPs, it results primarily from the content and services provided by the CAPs. CAPs are thus dependent on the connectivity of the ISPs' infrastructure, but also contribute substantially to building end-users' appreciation for the ISPs' internet access services.

In this context, some ISPs see themselves as platform operators in a two-sided market connecting CAPs to end-users and therefore want to make use of two-sided market pricing. This implies that e.g. CAPs, CDNs and other intermediaries as data providers on the other side of the market from the end customers would potentially also have to pay fees for the transit of their data to the end customer ISP. In contrast, CAPs in particular view the service of ISPs as a pure transport service and not as a platform service and thus merely as infrastructure to be able to offer their content to a broad mass of end customers. European retail ISPs in particular are currently arguing that large CAPs should participate in the investment costs of network expansion.[81] As already argued by the then AT&T CEO Ed Whitacre more than 15 years ago,[82] today the European ISPs in question still compare the behaviour of big tech players, which today account for the majority of traffic to end customers, with free-riding on their infrastructure. Therefore, from the point of view of these ISPs, these players should in future share in the costs of network expansion through direct payments to the end-customer ISPs (see black payment flows of CAPs in Figure 3-2). In this context, some ISPs argue that the strong competition in the access market does not allow sufficient margins to finance further network expansion to the desired extent without such participation.

81 ETNO (2021).
82 Herman (2006).

Figure 3-2: Two-sided payment flows



Source: Based on Krämer, J., Wiewiorra, L., & Weinhardt, C. (2013). Fig. 1 (p. 796).

Ultimately, however, the direct and indirect revenues of CAPs (and CDNs) also come from the end customer side (see blue payment/attention flows in Figure 3-2). Two-sided pricing by ISPs would thus correspond to a redistribution of rents from customers' combined appreciation of the bundle of internet connectivity and content. Moreover, CAPs are also in direct and strong competition with each other and also invest large sums in their (exclusive) local content offerings. Netflix, for example, says it will invest €500 million in German-language content alone by 2023.[83] Added to this are the investments in its own infrastructure (e.g. codecs, Open Connect). Furthermore, it is questionable why the concentration of data traffic on different CAPs and not the absolute level of data traffic in the network and at the network borders of the ISPs changes anything about the economic assessment and the demands of the ISPs concerned. The investments in network expansion are thereby based on the utilisation of the networks at peak times and not on whether this traffic volume originates from a few large CAPs or an atomistic number of small CAPs.

Furthermore, there is a difference between the possibility of being able to establish a two-sided price regime independently and a situation in which this is to be made mandatory by the regulator. Both the explicit exclusion of two-sided prices and the

83 Timpanist (2021).

mandatory introduction of two-sided prices can create inefficiencies from an economic perspective. Under the assumption of competitive markets, it is therefore questionable why a regulator should force a specific price regime on the existing interconnection markets, although this is already permissible with regard to the contractual freedom of all parties involved (e.g. in the form of paid peering or partial transit).

A change in the pricing regime for SPNP in Korea, for example, has led to a withdrawal of CAPs from the Korean market and a deterioration in the quality of their services. Domestic CAPs and end-users have been particularly affected. [84]

This chapter will therefore take a closer look at the position of the different players in the market and analyse them individually. In the forthfollowing chapter we will then discuss the causes for the developments presented in this chapter. Then, in chapter 5, we look at the relative power structure of the actors.

3.2 The position of the players in the market

3.2.1 End-user ISPs

The core business of retail ISPs (eyeball ISPs) continues to be the sale of broadband connections in combination with connectivity to the global internet. With the roll-out of FTTH networks, wholesale-only providers have also emerged in many countries, which exclusively offer (passive) broadband access in retail or wholesale and are not themselves active in the ISP business as integrated providers. There are only a few examples of large-scale integration of ISPs into their own content business. The most prominent is the acquisition of Time Warner by AT&T. In line with this is that ISPs (want to) create competitive advantages for themselves in the competition between ISPs with their own TV/VoD offerings as well as with exclusive content, e.g. in the area of sports. This does not create relevant competition to the large CAPs. This also applies to the cloud business. Compared to the large CAPs, the market shares of the telcos are rather modest. Due to their limited footprint, their services in this area scales significantly less than that of the CAPs. Their market opportunities are therefore limited to niches from the outset. There are no signs of a different trend in the future.

The core asset of ISPs in relation to CAPs is and will therefore remain the access to their own end customers. This termination monopoly remains an asset for both large and small ISPs. Here, the value of access to an individual ISP's network for a CAP naturally depends on the size of the individual ISP's network.

84 See in detail Section 2.2.1.

3.2.2 Backbone ISP

Backbone ISPs sell transit to other (smaller) ISPs or CAPs. In addition to eyeball ISPs that also act as backbone ISPs, there are specialised operators such as Level 3 and Cogent that primarily market backbone capacity as a business model.

The increasing density of internet traffic and internet topology is putting increasing pressure on the business model of transit providers. The large CAPs operate their own backbones and no longer rely on the services of the backbone ISPs to the same extent as before. Direct peering is increasingly substituting for transit. Above all, however, CDNs and especially on-net CDNs are substituting the business of the backbone ISPs. According to Abecassis et al. (2018), CAPs invested an annual average of USD 3.6 billion in transport and USD 2.2 billion in delivery in the period 2014-2017. While transport investments increased by only 30% compared to the same period in 2011-2013, delivery investments more than tripled. According to Telegeography, CAPs accounted for a larger share of international backbone capacity than internet backbone ISPs for the first time in 2016.[85] This trend is continuing. This is also evident in the fact that the large CAPs are participating more frequently and increasingly intensively in submarine cable projects or are now also providers of their own submarine cables.

In view of these market and traffic shifts, Dey and Yuksel (2019) see two development options for the backbone ISPs: either they attract enough traffic to their networks to be able to scale relevantly, or they or their backbone networks become takeover candidates, e.g. for the large CAPs.

Table 3-1 shows how the independence of the networks and their reachability developed in the period from September 2015 to September 2020. Hierarchy-free reachability here refers to the direct connection to the relevant target networks, without passing through the networks of tier-1 or tier-2 backbone ISPs, as well as the network of the transit provider of the target network.[86] Google already had a hierarchy-free reachability of 81.7% in 2015 and was able to increase this to 86.9%. Level 3 has retained its leading position. Microsoft leaped from position 62 to position 4 (84.6%) and Amazon from position 206 to position 18 (75.0%). In 2020, only the telcos NTT, Colt, Telia and Swisscom are still represented in this top 20.

---

85 Telegeography, after Abecassis et al. (2018), p. 29.
86 Arnold et al. (2020), p. 236.

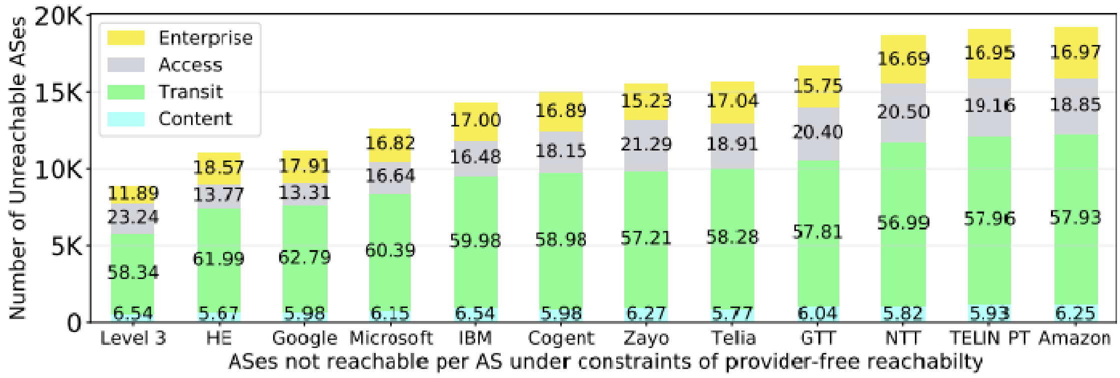
Table 3-1: Hierarchy-free accessibility for the top 20 networks (Sept. 2015-Sept. 2020)

2015			2020		
#	Network (AS)	Reachability (%)	#	Network (AS)	Reachability (%, % change)
1	Level 3 (3356)	43,413 (83.4%)	1	Level 3 (3356)	61,154 (90.2%, 6.8)
2	Google (15169)	42,347 (81.7%)	2	HE (6939)	58,981 (87.0%, 6.2%)
2	HE (6939)	41,876 (80.8%)	3	Google (15169)	58,922 (86.9%, 5.2%)
4	Cogent (174)	39,113 (75.5%)	4	Microsoft (8075)	57,357 (84.6%, 22.0%)
5	StackPath (12989)	39,068 (75.4%)	5	IBM (36351)	55,714 (82.2%, 10.4%)
6	WV Fiber (19151)	38,756 (74.8%)	6	Cogent (174)	55,049 (81.2%, 5.7%)
7	RETN (9002)	37,796 (73.0%)	7	Zayo (6461)	54,489 (80.4%, 11.5%)
8	NTT (2914)	37,543 (72.5%)	8	Telia (1299)	54,324 (80.1%, 8.9%)
9	IBM (36351)	37,203 (71.8%)	9	GTT (3257)	53,388 (78.7%, 8.7%)
10	IPTP (41095)	37,048 (71.5%)	10	SG.GS (24482)	53,157 (78.4%, 9.7%)
11	Telia (1299)	36,906 (71.2%)	11	COLT (8220)	52,256 (77.1%, 12.9%)
12	iiNet (4739)	36,846 (71.1%)	12	G-Core Labs (199524)	51,820 (76.4%, 27.4%)
13	Init7 (13030)	36,814 (71.1%)	13	NTT (2914)	51,374 (75.8%, 3.3%)
14	MTS PJSC (8359)	36,786 (71.0%)	14	Wikimedia 14907)	51,204 (75.5%, 25.7%)
15	Telstra (10026)	36,322 (70.1%)	15	Core-Backbone (33891)	51,110 (75.4%, 12.7%)
16	GTT (3257)	36,238 (70.0%)	16	WV FIBER (19151)	51,083 (75.3%, 0.5%)
17	PCCW (3491)	36,109 (69.7%)	17	TELIN PT (7713)	50,919 (75.1%, 18.6%)
18	TDC (3292)	36,001 (69.5%)	18	Amazon (16509)	50,867 (75.0%, 17.3%)
19	Swisscom (3303)	35,772 (69.1%)	19	Swisscom (3303)	50,758 (74.9%, 5.8%)
20	Zayo (6461)	35,686 (68.9%)	20	IPTP (41095)	50,606 (74.6%, 3.1%)
62	Microsoft (8075)	32,436 (62.6%)			
206	Amazon (16509)	29,905 (57.7%)			

Source: Arnold et al. (2020), p. 237.

Figure 3-3 shows the opposite picture of how many ASes cannot reach the top 12 backbone networks and how this is divided between the corporate, access, transit and content networks. Google, IBM and Microsoft focus their peering efforts primarily on reaching access networks. These data show that large CAPs today only need to reach a small part of the ASes via transit.

Figure 3-3: Number and distribution of non-accessible ASes of the top 12 operators



Source: Arnold et al. (2020).

3.2.3 CAPs

After transferring content between data centres and across international backbones, CAPs deliver their content to end-users via ISPs' networks. Traffic handover takes place at public IXPs to a large number of ISPs and at private peering points directly with individual ISPs if the relevant traffic volumes suffice.

Already in 2017, BEREC reported that the large CAPs were investing heavily in their own network infrastructure in order to handle traffic more efficiently, reduce dependency on others, gain more flexibility for their own capacity upgrades and improve the quality of service delivery to the end customer.

In order to deliver their content efficiently and in high quality to end customers, CAPs are investing in their CDN infrastructure and in more efficient video streaming technologies.

CAPs are now not only increasingly participating in international submarine cable projects, they are now also investing independently in their own submarine cable projects. In 2018, Facebook, Amazon and Microsoft either owned or leased more than 50% of submarine cable bandwidth.[87] In 2019, Google alone owned six active submarine cables and plans to build another eight in the next two years.[88] By investing in the latest cable technology, CAPs gain the lowest transmission costs, giving them a (cost) advantage over most backbone ISPs. It also gives them increasing control over the network design and management of their backbone capacity.

87 Mozilla Foundation (2019).
88 Mozilla Foundation (2019).

However, the massive investments in the delivery infrastructure of CDNs also make CAPs much more independent of the ISPs' network investment decisions. By placing their cache servers deep in the ISPs' networks, they rather control the quality of service themselves and are not dependent, or are at least less dependent, on the ISPs' upgrade investments. Furthermore, they increase transmission efficiency so that content has to be routed less and less via international backbones. Looking at ISPs' networks and CAPs' infrastructure as a unit, this development reflects an efficient overall optimisation of the hosting, transport, delivery and access network infrastructure. The access to the eyeballs provided by the ISPs remains as the last bottleneck over which CAPs today have no control. Apart from a few demonstrative individual projects such as Google Fiber[89], no relevant projects for a vertical integration of CAPs into the access network infrastructure of the ISPs have been identified so far. They also currently have no levers to motivate ISPs to upgrade the capacity of their access networks. However, the transformation of access networks into FTTH networks seems to be an irreversible trend worldwide. In this respect, the current strong investment efforts of ISPs and infrastructure investors as well as the related government subsidy programmes are in line with the CAPs' interest in high performing access networks.

It is true that the number of public peering points accessed by CAPs has risen sharply. However, the share of traffic via private peering has increased significantly more. While the number of public peering points accessed by CAPs more than tripled from 2014 to 2018 (to 1096), the number of private peering points increased by 88% (to 544). [90]

In addition to in-house CDNs, large CAPs such as Amazon, Alibaba, Google and Microsoft also operate commercial CDNs to support services used by their cloud customers.[91]

CAPs pursue an open peering policy, do not charge for peering and only pay network fees to ISPs in exceptional cases. The interaction of the networks and infrastructures of ISPs and CAPs today is intensive and cooperative. Therefore, the payment of network charges to ISPs plays a rather minor role compared to the strategic investments of CAPs in infrastructure from hosting to transport to service delivery. A regime of network charges comparable to the requirements in South Korea would - like any new regulatory intervention - lead to a change in the previous equilibrium and require an adjustment path to a new equilibrium. This would have at least a temporary disruptive effect on the efficient functioning of the internet. The example of South Korea shows that these measures can thus have a negative impact on the quality of the content delivered and thus on consumers. In view of the considerable investments in their own infrastructure system, it is to be expected that CAPs would resist a change in the current balance. Moreover, ISPs would only have a chance to change the existing balance if they acted

89 Google (2021b).
90 Abecassis et al. (2018), p. 34.
91 Abecassis et al. (2018), p. 37.

in a coordinated manner at the European level and not only at the national level. In that case, they would avoid competitive damage for themselves and could limit or restrict CAPs' circumvention activities.

3.2.4 CDNs

Already in 2017, BEREC highlighted the trend towards an increasing economic relevance of CDN for IP traffic.[92] Based on the traffic development of the past years, we have shown in Section 1.5 that CDNs now represent the dominant form of IP service provision. BEREC stated in 2017 that CAPs were increasingly pursuing a multi-CDN strategy and relying on several CDNs for resilience reasons. In this respect, the market at the time consisted of a diverse number of players: specialised CDN companies, CAPs' own (in-house) CDNs and CDN services from telcos.

There have been significant shifts in this structure. The most dynamic development has been in in-house CDNs of large CAPs. Today, all large CAPs operate their own CDNs. As a rule, these deliver (by far) most of the CAPs' content. Netflix's Open Connect CDN delivers (almost) 100% of Netflix's traffic and content. The integration of the CDN function and full control over their own CDN has apparently dominated the resilience benefits of a multi-vendor strategy for the large CAPs. Given the traffic volumes of these CAPs, there also do not seem to be any scale disadvantages on the cost side compared to specialised CDN providers.

As an example, Netflix's CDN approach is briefly described below. Netflix has built up and further developed its own CDN "Open Connect" over the last 10 years. The scale of the investment in its own CDN is demonstrated by the fact that Netflix has invested USD 10 billion in this infrastructure over the last 10 years. Compared to 12 billion USD invested in content alone in 2020, the CDN investment is of a relevant magnitude, but does not change the dominance of content costs in characterising Netflix's business model as a CAP and not (primarily) as an infrastructure operator. Open Connect consists of a global backbone and about 17,000 content cache servers in 158 countries, also referred to as Open Connect Applications (OCA). Each OCA stores nearly all of Netflix's content. The OCAs are located in Public Internet Exchanges, in multi-tenant data centres or directly in ISP networks. Network development is characterised by a steady reduction in the distance to the end user. The density and depth of the network is illustrated by the fact that Netflix operates cache servers at 117 locations in Germany. In the UK, Netflix operates its densest network at as many as 150 locations. At each location, they operate 2-16 servers. In Germany, Open Connect works directly with about 50 ISPs. This means that Netflix's CDN is also directly interconnected with regional and (large) local ISPs. In this respect, the traffic requirements for direct interconnection are relatively low.

92 BEREC (2017), pp. 8 f. and pp. 36 ff.

Netflix considers the relationship with the ISPs to be cooperative and even symbiotic. The positioning of the cache servers is done as part of a joint network planning. Netflix transfers ownership of the servers located in the ISP's network to them. The operation and maintenance of the servers is carried out by and at the expense of Netflix. The amount of content is fixed, it is played off-peak to the cache servers every night. According to Netflix, an ISP that installs Open Connect servers in its network serves on average more than 95% of Netflix traffic locally, without transport via long-distance interconnections.[93] This reduces the respective ISP’s network costs, for example through reduced transit capacity, and reduces the risk of network congestion on the part of the ISP's infrastructure. Netflix reports that BT said it achieved 60% savings in core network costs in 2018 by localising content deeper in the network. Without being able to verify this, Netflix estimates that ISPs installing Open Connect servers directly on their networks would have saved USD 1.2 billion in network costs in 2020.[94] ISPs generally bear the costs of collocation and power supply. In 2021, more than 1,000 ISPs had made use of this option and installed OCAs in their networks.[95] This economic consideration may be different for ISPs who have been able to enforce charges for transit into their networks against CAPs. Here, the efficiency gains from local delivery of content and the associated quality gains are offset by revenue losses from the interconnection business.

Netflix does not charge peering fees to ISPs. As a rule, this also applies to the ISPs. From Netflix's point of view, this configuration has the great advantage that the ISPs have no off-net traffic with Netflix for which they would have to pay for backbone capacity, interconnection and transit.

As the only exception worldwide, Netflix maintains a paid peering relationship with DT, which the latter, however, evaluates as a transit relationship. The Open Connect servers are also not installed in DT's network. Rather, the traffic is handed over at five central network crossings in Germany.

Public peering at IXPs no longer plays a major role for Netflix. Only very small providers are reached here via a "catch-all" strategy, for which participation in Open Connect does not (yet) seem worthwhile or necessary. Globally, only 3.5% (3.1% in Germany) of Netflix traffic is transferred to IXPs. Furthermore, public peering is a fallback option in case of bilateral problems. Before Netflix could rely on its own Open Connect CDN, interconnecting at IXPs was relevant for Netflix. If an OCA is installed at an IXP, Netflix retains ownership of it and also bears the costs of power consumption, collocation, cross-connect fees and the like. In total, Netflix was present at 80 IXPs in more than 25 countries in 2021.[96]

93 Netflix (2201b).
94 Netflix (2021b), p. 6.
95 Netflix (2021a), p. 21.
96 Netflix (2021a), p. 21.

Breaking down this trend towards in-house CDNs, this also means that the business of specialised CDN providers has developed less strongly than total CDN traffic. Abecassis et al (2018) expect that in 2021 48% (32% in 2016) of global internet traffic will be in-house CDN traffic from CAPs. Commercial CDN traffic is expected to account for 22% in 2021 and non-CDN traffic for only 30% (48% in 2016).

There are clear indications that the telcos have not been able to develop a successful CDN business of their own. While some telcos are said to have tried to develop their own CDN, these attempts do not seem to have led to any discernible market success. Often telcos do offer CDN services, but they provide them in cooperation with partners.

Another market trend BEREC identified in 2017, but underestimated in its importance for the peering and transit markets, is the trend towards on-net CDN, i.e. the positioning of the CDN's cache servers directly in the ISP's network. By far the majority of ISPs now maintain this on-net CDN relationship with the large CAPs and the large specialised CDN. Even small and medium-sized ISPs now have this network cooperation. It typically consists of the CDN / CAP providing, installing and maintaining the cache server. Of course, it is also responsible for updating the content. The ISP typically provides the spatial accommodation and power supply. The high and (spatially) deep penetration has structurally changed the network configurations and peering and transit relationships of the participants in the long term. Especially larger ISPs save (their own) core network costs through on-net CDNs and, depending on the depth of the positioning of cache servers in their network, also save capacity in the aggregation network. However, they may also lose transit revenues and possibly also revenues from paid peering due to the greater regionalisation/localisation of traffic. Smaller ISPs save transit fees and, to a relatively lesser extent, their own network costs if the caches are positioned directly in their network. The advantage for both sides of the market is the improvement/assurance of the quality of transmission for the end customer. CDNs minimise the number of routers and networks that content has to pass through on its way to the end customer. This minimises the risk of congestion and generates a high level of quality. In our estimation, this is also the main motivation for CAPs to invest in CDN, rather than the saving of transit fees.

Doan et al. (2021) measured this quality improvement through Netflix's CDN over a period of three years (2016-2019). Doan et al. observed that the Netflix Open Connect servers are reachable on-net in 6 IP hops in the ISP's network. This can shorten the IP path length by 40% for IPv4 and by 60% for IPv6. Across both address families, this reduced the TCP connect time by 64%. While a TCP connection to a Netflix Open Connect server took ≈25-27 ms in 2016, in 2019 this was only ≈15-16 ms with similar latency for both address families. The throughput achieved also increased by a factor of three when ISPs used caches on-net to stream content.

3.2.5 IXP operators

We have already shown by means of traffic development in Section 1 that the use of IXPs for public peering has decreased relative to other forms of interconnection. The traffic shift towards private peering is primarily driven by CAPs. While 10 to 15 years ago they exchanged more than 50% of their traffic at the IXPs, today it is significantly less than 10%. DE-CIX otherwise assumes that just under 25% of all IP traffic in Germany is exchanged via DE-CIX. DE-CIX has a relatively greater significance here than other IXPs in Europe due to Frankfurt's central role as a focal point for all non-European traffic. At DE-CIX, traffic roughly doubled between 2015 and 2020. The annual growth rate was around 15%. Since COVID-19, growth has increased to 20-30%. The higher level has persisted so far.

Nevertheless, the CAPs in particular clearly emphasised in our interviews that IXPs continue to play a central role and task for a functioning and open internet. Especially for the traffic exchange of small ISPs and CAPs, IXPs continue to play an essential role. In addition, their function as a central hub for traffic exchange has changed. The IXPs are increasingly taking on the role of a back-up or resilience operator for the large players (CAPs, ISPs). IXP capacities are used to cover traffic peaks, absorb surprising traffic loads or take over traffic in case of POI failure in private peering. Furthermore, they take over traffic until POIs are further expanded. According to DE-CIX's assessment, the IXPs are quite capable of sufficiently monetising this back-up function. Although prices at DE-CIX have also fallen continuously, they have fallen less than the growth in traffic.

The IXPs are preparing for the strongly increasing regionalisation/localisation of traffic by setting up/expanding further internet exchanges. For example, DE-CIX already operates additional sites in Hamburg, Düsseldorf and Munich. The plan is to have completed the expansion to 11 locations in all German metropolitan regions by the end of 2022.

The business model of the IXPs has also evolved in recent years due to the fact that (especially) large companies themselves are directly present as users at the IXP and exchange traffic there. This applies, for example, to companies in the automotive industry.

Another strategic development of DE-CIX's business is to develop its own cloud business. The niche for DE-CIX here is to provide virtual connections for a direct interference-free path to the cloud. This strategic further development of the business is complementary to the direct presence of large companies at DE-CIX.

DE-CIX is also facing increased competition from multi-tenant data centre operators, as ACM has also noted for the Dutch market. A particular competitive challenge for public IXPs in the Netherlands is that the incumbent telco KPN has built its own IXP NL-IX there and has shifted peering capacity from AMS-IX to its own IXP. KPN’s own IXP therefore becomes a tool for KPN to monetize the intially free peering at the public IXP.

DE-CIX is also countering the slower development of its domestic business by increasing the internationalisation of its business. DE-CIX is now active as an operator of IXPs at around 30 locations worldwide, with a focus on Europe. Three models are being pursued. In Dubai, DE-CIX operates the IXP on behalf of a local operator. DE-CIX is fully responsible for operating IXPs in Madrid, Palermo and Turkey, for example. Furthermore, DE-CIX is active in cooperation with national partners, e.g. in India.

Following Sowell (2020), the development of IXPs over time can be described as follows: IXPs were established in the late 1990s to keep local traffic local. Small and medium-sized networks connected to the global internet at the IXP via transit operators. IXPs also provided a platform for bilateral peering to reduce costs and legacy. In their business model, IXPs used to provide, as they do today, a "platform-as-a-service" that allows networks to publicly peer with other networks. Today, IXPs have further evolved into neutral market exchange platforms alongside CAPs' platforms.

It can thus be said that IXPs continue to play a significant role in the functioning of an open internet. However, contrary to BEREC's expectations in 2017, their importance as traffic exchange points has decreased. Private peering and on-net CDN traffic has increased significantly more than the traffic handled by IXPs.

At the same time, it can be seen that IXPs are responding to the changing trends in the market and seem to be managing this commercially successfully. This applies to the greater regionalisation of traffic, the increasing competition from multi-tenant data centre operators and the greater importance of cloud business. The IXPs' platforms also seem to attract new customer groups with new product offerings.

These developments make it clear that the market players have been able to adjust and adapt to the changes in the market so far. However, no automatism for the future can be derived from this. Nonetheless, it must be taken into account that vertical integration means that pure intermediaries (e.g. IXPs) in particular have to adapt more strongly and quickly than other market players. The fact that this has worked so successfully so far speaks for the fact that there is a high flexibility and adaptability in this area.

4 Central factors influencing market development

4.1 Technological changes

The most significant technological changes for peering and transit are related to CDNs. Their decentralised location and performance have permanently changed the structure of internet traffic, as we explained in detail in Section 1.2. Doan et al. (2020) have shown how on-net CDNs have significantly reduced the latency of content transmission and significantly improved the quality perceived by end users.[97]

Further development progress is foreseeable here, which will make the use of CDNs even more attractive. Goetz (2019) highlights further potential for increasing performance. Today, CDN providers can only evaluate data on POP performance by collecting log files. The volume of this data and its update pattern make problem solving, system upgrades and quality assessment difficult. Therefore, in the future, CDNs will rely on predictive analytics and algorithms to anticipate behavioural changes based on artificial intelligence. These technologies, based on the OSI model, can replace the Border Gateway Protocol (BGP), which currently routes internet traffic. The largest internet companies in the world are working on this.

Data centres are by far the largest block of investment for CAPs, leading to dynamic progress. However, technical changes in hosting also have repercussions for networking.

CAPs work with telcos and equipment manufacturers to further develop network technologies. This is done, for instance, in the Open Networking Foundation (ONF), which is an open-source platform for defining standards and developing and promoting future network transformation.[98] For example, an open-source Software Defined Networking (SDN) switching platform is being developed in the "Stratum" project. The initiators were Google and Tencent. Other participants include manufacturers and telcos such as China Unicom, NTT and Turk Telekom.

4.2 Change in network structures

The main changes in the overall global architecture of the internet and telecommunications interconnection are caused and driven by the massive expansion of own backbone and delivery infrastructures by the CAPs. In the 2012 report on IP interconnection, BEREC already reported on a flatter and less hierarchical structure of the internet. Even then, it became apparent that less and less traffic would be routed via

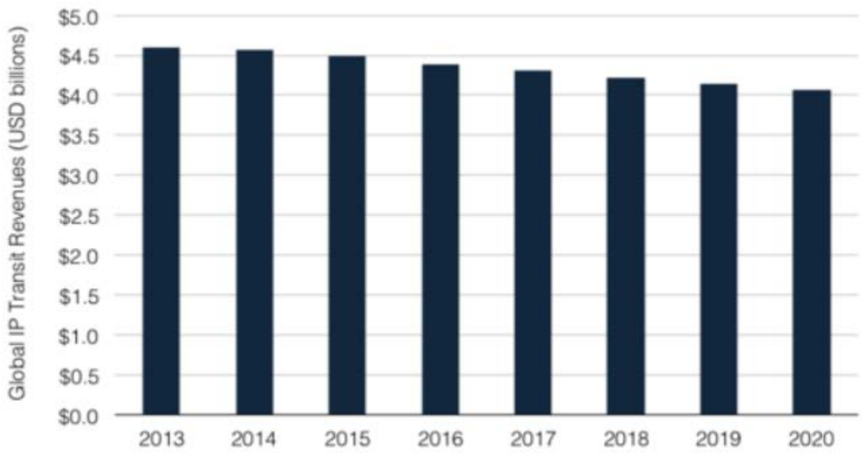
97 See Section 1.2.4.
98 Abecassis et al. (2018), p. 42.

global Tier 1 backbone ISPs. Instead, direct private and public peering would increase. As a result, the architecture has become more meshed over time and thus less hierarchical (flatter).

In the subsequent report from 2017, BEREC highlighted the CAPs' increasing investments in their own backbone and delivery infrastructures. CAPs' actual investments underline this assessment and expectation. CAPs' infrastructure investments are clearly dominated by hosting investments at 92%.[99] Investments in transport averaged $3.6bn (=4.8%) from 2014 to 2017. Delivery infrastructure investment was USD 2.2bn p.a. (=2.9%), but had the highest growth of +127% compared to the previous period (2011-2013). In the area of transport infrastructure, significant increases in investments in submarine cables in particular have been observed. CAPs are now initiators and promoters of submarine cable projects and no longer just co-investors.

This increasing meshing of the internet and the CAPs' investment in their own backbone infrastructure means that the backbone networks of the Tier 1 operators and transit over these networks are becoming relatively less important.[100] They are no longer the central backbone of the internet and have lost their historical role in this respect. They are losing their role as an essential carrier of internet traffic and are increasingly taking on the role of resilience and back-up infrastructure.

Figure 4-1: Global IP Transit Revenues (2013-2020)



Source: Marcus (2014).

99 In the period 2014 to 2017 according to Abecassis et al. (2018).
100 Arnold et al. (2020).

Arnold et al (2020) have quantified the extent of bypass of Tier 1 networks by the major cloud providers. They show that cloud providers can reach more than 76% of the internet without backbone networks from Tier 1 and Tier 2 providers. According to Arnold et al. (2020), there are only 174 AS networks that Google cannot reach directly, without the participation of transit providers. Reachability is thus comparable to that of most Tier 2 operators. Transit networks lose revenue, traffic volume and importance as a result. Figure 4-1 shows a slow but steady decline in transit revenues since 2013. This represented a forecast from 2014. We expect this trend, which Telegeography anticipated in 2014, to have accelerated in recent years. In addition to investments in own backbones, the massive investment of cloud providers in globally distributed huge data centres is also responsible for this trend. In the process, the cloud infrastructure of Amazon, Google, IBM and Microsoft is also being used by many CAPs.

4.3 Cost and price development

Moore's Law still applies to the cost of essential elements of the Internet's hosting, transport and delivery infrastructure. With each new generation of equipment, the cost per unit decreases significantly. Furthermore, the relevant product life cycles are becoming shorter and shorter. As a result of this technological progress, combined with the economies of scale of steady traffic and volume growth, the relevant costs continue to fall. In this respect, the cost trends identified in detail by Marcus (2014) continue to apply. Insofar as competition prevails in the relevant markets, these cost trends are reflected in the prices. This is evident in the case of transit and backbone capacities.

The ongoing cost and price dynamics continue to generate increasing economies of scale for the Internet's infrastructure systems. This creates competitive disadvantages for smaller ISPs/CAPs if they are in direct competition with larger ones. Providers that fail to participate in traffic growth may lose economies of scale. However, economies of scale and their exploitation also influence the make-or-buy decisions of large players. If their business volume increases, they can more easily use the economies of scale of infrastructure systems themselves and avoid dependency on market services.

This analytical background serves as evidence for the influence of cost dynamics and economies of scale on a number of the structural changes in the market described in this study. This applies, for example, to CAPs' own backbones, to the trend towards direct peering and to on-net CDNs. The dynamics of increasing economies of scale demand functioning market solutions for smaller players to maintain their competitiveness and thus diversification in the market. Market elements such as the IXP, commercial CDNs, transit providers and platform-as-a-service therefore play a central role in the competition between players with different market positions.

4.4 Transport and services

The sustained growth of internet traffic and the resulting volumes continue to shape the dynamics of the internet's architecture. The second defining factor is the dominance of video streaming and cloud-based services. Both factors are driving CAPs' transport and delivery infrastructure development. Derived from this, these factors have continuously shifted the relation of interconnectionin form of transit, private peering and public peering. Furthermore, with the traffic- and service-driven development of on-net CDNs, a very direct and cooperative interaction between CAPs and ISPs has emerged. It is an expression and prerequisite for a highly efficient architecture of the internet and the interaction of the networks.

This evolved architecture and interaction of the networks has passed the stress test induced by the new traffic spikes during the COVID-19 pandemic, unlike the physical supply chains. The networks were able to cope with traffic increases of 20 to 30% without any discernible major disruptions. Of course, this was also possible because the daily load curve shifted and became more even. However, the networks were also able to cope with an 18% higher increase in upstream traffic.[101] Particularly drastic was the 200% increase in VPN traffic due to the heavy reliance on home offices.

4.5 Changes in the conditions of the legal and regulatory framework

Taking a closer look, nothing has changed in the legal and regulatory framework for IP interconnection in Europe. The bill & keep settlement system is still practised in the market. ISPs and CAPs have to agree technically and commercially on the conditions for transit and peering bilaterally. Even more detailed arrangements for on-net CDNs are made commercially and remain unregulated. This applies to the locations of traffic handover as well as the level of transit prices and whether peering takes place in a settlement-free or paid context. Our survey of NRAs also confirmed that there have only been a few cases of NRA intervention into the contractual freedom of market actors. The main exception is the intervention of the competition authority in the peering dispute between Init7 and Swisscom in Switzerland.[102] Here, the competition authority, confirmed by a decision from the highest court, found that Swisscom was exploiting a dominant position in peering and ordered the regulatory authority to regulate the conditions of interconnection. Besides that, some NRAs have become involved in dispute resolution.[103]

If one takes a broader view, the framework conditions have also indirectly changed for the wholesale relationship between CAPs and ISPs through the European regulations

101 According to Feldmann et al. (2021).
102 See Section 5.2.1.1.
103 See in detail Section 5.2.

on network neutrality. EU Regulation 2015/2120 of the European Parliament and of the Council of 25 November 2015 established key principles on access to an open internet. These have since been further specified by BEREC guidelines for uniform application by NRAs in the EU.[104]

Although this regulation primarily focuses only on the protection of end-users, the rules established also have retroactive implications for IP interconnection. According to Article 3 (3), ISPs must treat all traffic in a non-discriminatory manner, regardless of sender and receiver. In its 2012 report on IP interconnection, BEREC highlighted that interconnection agreements between networks have no direct relation to net neutrality as long as data flows are treated equally at the wholesale level.[105] Nevertheless, deviations from net neutrality could also have repercussions on the wholesale level. Similarly, a disruption of interconnection at the wholesale level can also lead to end-users not reaching all destinations of the internet, with lasting implications for net neutrality as some of the following examples show.

In two merger decisions, each involving (large) cable network operators, the EU Commission as competition authority imposed remedies on the peering and transit policy (in the form of voluntary commitments to approve the merger). The intention of these conditions is to prevent abuse in transit and peering that could result from the integrated business model of an ISP and the distribution of its own content.

In March 2014, the European Commission was notified of Liberty Global's plan to acquire the Dutch cable network company Ziggo. Due to possible restrictions of competition in downstream markets of audiovisual sports TV services, a re-evaluation was carried out by the Commission in 2018. The reason for the investigation at that time was the assumption that there could be an incentive to foreclose the market due to the existing distribution platforms of the combined companies and the ownership structure of Liberty Global. An ISP that sells its service via cable to end customers and at the same time also has visual services in its portfolio is in (potential) competition with other audiovisual pay content. Accordingly, in the context of the re-evaluation, the European Commission again identified, among others, the market for the provision of premium video services as being affected by the takeover.[106] The European Commission found indications of a willingness to use bargaining power in licences in order to reduce the penetration of OTT services.[107] Similarly, the company could influence the penetration of services as an ISP. This was demonstrated by the peering dispute presented in Section 5.3.3 which, while not directly aimed at anti-competitive measures in video streaming, resulted in a perceptible reduction in Netflix's quality of service.

104 BEREC (2020).
105 BEREC (2012). pp. 4ff.
106 European Commission (2018) p. 27.
107 European Commission (2018) p. 101.

In the course of its investigation, the Commission had found that Liberty only wanted to offer free and high-quality peering if the OTT simultaneously exclusively distributed TV and content services to Liberty's customers. The Commission saw this as an inadmissible mixing of the technical role of providing OTT services and TV providers restricting the decision-making of OTT services. The European Commission concludes from Liberty Global's contracts that Liberty Global, through the application of its peering policy, is in a position to influence the quality of specific services by failing to expand the capacity of interconnection to certain transit providers.[108] As a proposal to remedy this incentive, Liberty Global already committed in the first review in 2014 to maintain three interconnection routes via transit partners into its network, which must be kept free of congestion at all times. In the re-evaluation, the European Commission saw no need to extend this obligation, as in 2018 there was no evidence of limited penetration of OTT services involving Liberty Global and thus the purpose of the former imposition was fulfilled. This is consistent with the CAP developments discussed in Section 5.3.3, but shows the former competitive relationship between ISPs and CAPs. What is interesting here is the possibility for ISPs to get an impression of which transit partner is connected to any CAPs via routing tables and to use this information as leverage by not upgrading capacities (i.e. undersizing transition points at the network edges). This could have implications downstream for incentivising paid direct peering, even if it does not limit the spread of CAPs.

In the merger of parts of Liberty Global and the Vodafone Group in 2018, Vodafone also gave a similar assurance.[109] In the event of a merger, Vodafone promised to provide three non-congested routes from transit providers to the newly merged core network. The daily peak load was not to exceed 80%, which has to be verified by a trustee, who additionally verifies the list of potential transit partners. The background here was also a potential weakening of the market position of OTT services vis-à-vis Vodafone's own audiovisual services, as the European Commission explained in its decision. Vodafone's commitment is valid for 8 years, which the Commission assumes is a typical cycle of strategic decisions in the OTT business.

108 European Commission (2018) pp. 118f.
109 European Commission (2019).

5 Relative power structure

5.1 Business models and strategic positioning of the players

First of all, this chapter outlines the business models of the different players before looking at the relative power structure of the players. In this context, it can basically be stated that CAPs and ISPs are mutually dependent on each other. ISPs provide the connectivity of end customers to the internet, from which CAPs benefit indirectly through accessing the target group. However, the availability of a rich offer of online-based services and content also increases the attractiveness of a (fast) internet connection, which in turn can have a positive effect on the number and/or price of marketed internet connections.

The revenue models of end-user ISPs in Germany differ in their orientation between mobile and fixed networks. In mobile networks, customers are primarily asked to pay on the basis of the monthly usable data volume for their mobile internet connection, while the classic telecommunications services in mobile telephony are already frequently billed in the form of a flat rate. In the context of fixed broadband connections, flat rates also represent the most widespread business model for connectivity to the internet. However, the price level is primarily determined by the maximum available bandwidth and not by the usable data volume. The charges from end customers represent the main source of revenue for end-customer ISPs.

The business models of CAPs, on the other hand, are primarily based on the attention of end customers. The monetisation of this attention can take place both through advertising revenue and direct fees. These fees can be charged regularly at certain intervals (e.g. subscription) or per transaction (e.g. rental). In this context, customers' willingness to pay is determined by their interest in and duration of consumption of a CAP's content. Just as the construction of a network generates high sunk costs, the production of new content in particular also generates high one-off costs. In contrast, localisation (e.g. dubbing, subtitles) and digital distribution incur relatively low variable costs. However, this cost structure mainly applies to professionally produced content (e.g. series, films), as user-generated content (e.g. YouTube) does not have to be pre-financed directly by the CAP. In this case, the risk of refinancing the production costs lies exclusively with the users, who only participate in the advertising revenue of the platform when their content is distributed.

The costs for CDNs and transit connections, on the other hand, are usually dependent on the transmitted data volume. This means that the comparatively fixed revenues on the end customer side are offset by variable costs on the backbone connectivity side, which depend on the intensity of use of the end customers. However, there is of course also the possibility for CAPs to replace these variable costs with fixed costs through a high proportion of peering. This is the greatest incentive for CAPs to build their own CDN structures and conclude peering agreements.

However, the development of their own CDN and increased accessibility of large CAPs such as Netflix via settlement-free peering also mean the loss of revenue for ISPs through paid peering or (partial) transit. In the USA, the large retail ISPs decided in 2014 in such a situation not to further expand capacity at the relevant transfer points.[110] As a result, over time, there were increasingly frequent bottlenecks and unsatisfactory accessibility of the streaming offer for paying Netflix subscribers at the ISPs concerned.[111] At the time, this conflict was waged to the detriment of consumers, as Netflix and the ISPs concerned accused each other of being responsible for the situation. Ultimately, Netflix was able to reach an agreement with these ISPs on direct paid peering. This agreement subsequently restored the usual quality of service for end customers.[112]

In a similar dispute between the German hosting provider Hetzner and Deutsche Telekom, Hetzner is quoted by the industry portal teltarif.de as saying: "Daher beobachten wir mit wachsender Sorge DSL- und Kabelanbieter, welche einerseits selbst keine offene peering policy betreiben, aber andererseits auch nicht mit ausreichender Kapazität zu anderen Tier-1-Carriern angebunden sind." *[We are therefore observing with growing concern DSL and cable providers which, on the one hand, do not have an open peering policy themselves, but, on the other hand, are also not connected to other Tier 1 carriers with sufficient capacity*].[113] In this context, Hetzner complained that without payment the interfaces would be “am Kapazitätslimit betrieben” [operated at the capacity limit]. After Hetzner had optionally passed on these fees to its customers for several years (tariff option) in order to be able to offer sufficient connectivity to the Deutsche Telekom network on request, a direct interconnection with costs was agreed in March 2020. According to Hetzner's own statement, the decision was made to take this step because customers “…mit massiven Erreichbarkeitsproblemen zu kämpfen hatten und sich deshalb nach Alternativen umsehen mussten“ *[...were struggling with massive accessibility problems and therefore had to look for alternatives*].[114]

---

110 Engebretson (2013).
111 Wang & Ma (2020).
112 In a contribution by the Institute for Internet and Society, an interview partner is quoted on this topic as follows, cf. Meier-Hahn (2021): „[…] wenn ich etwas unternehme, das so aussieht, als würde ich eine Aufrüstung erzwingen oder ein Netz zur Zahlung zwingen, dann ist das potenziell ein Bereich, der vor allem in sozialer Hinsicht eher negativ ist, und potenziell auch aus regulatorischer Sicht. [...] Es ist also besser, wenn ich inkompetent erscheine, als wenn ich aktiv versuche, Einnahmen zu erzielen. Wenn ich also nicht aufrüste und nur wenig Kontakt zu einem Unternehmen habe, muss ich nur warten." [[...] if I undertake something that looks like I am forcing an upgrade or forcing a network to pay, then that is potentially an area that is rather negative, especially from a social perspective, and potentially also from a regulatory perspective. [...] So it's better if I appear incompetent than if I actively try to generate revenue. So if I don't upgrade and have little contact with a company, I just have to wait.] This quote illustrates that network operators are well aware of the potential regulatory implications and impact on end-users and may view undersized interconnection points as a soft solution to put pressure on CAPs.
113 Kuch (2015).
114 Hetzner (2020).

Ultimately, these and comparable cases initially document a perceived imbalance of relative market power. This was subsequently explored economically between the parties involved during the peering negotiations in the case of Netflix in the USA. Since ISPs and CAPs are in an interdependent relationship, the mere threat of downgrading a peering partner to a customer does not seem very credible from the perspective of the other party. Such actions therefore demonstrate that a party is indeed willing to inflict damage on its own business (and thus on its own end customers), since from its point of view a subsequent settlement is considered likely and the long-term profit to be expected from the new customer relationship is estimated to be profitable in relation to the short-term damage. Moreover, this expected profit does not only have to result from the individual consideration of a specific interconnection, but can rather also be subordinated to the credibility of a chargeable interconnection policy and thus future expected or maintainable profits of all interconnection customers. One interviewee describes the situation as follows: „[…] wenn ich das Peering wirklich brauche und Sie die Leitung kappen, bin ich ein Kunde. Logischerweise bin ich mehr auf Sie angewiesen als Sie auf mich. Das haben Sie bewiesen, indem Sie die Leitung gekappt haben." [*[...] if I really need the peering and you cut the line, I am a customer. Logically, I am more dependent on you than you are on me. You have proven that by cutting the line.]*[115] So as long as it remains pure threats or complaints, the internal evaluation of an existing peering agreement seems to shift to the disadvantage of one party, but there is still no need to force the other party to the negotiating table by cutting the connection or imposing capacity restrictions. The following sections will therefore analyse whether the identified relevant disputes are to be regarded as temporarily necessary frictions or whether the potential impact on end users must be judged as too serious and thus justify e.g. arbitration by the regulator.

5.2 IP interconnection disputes in Europe

5.2.1 Disputes between ISPs

5.2.1.1 Init7/Swisscom in Switzerland

The ruling of the Swiss Federal Administrative Court (2020) of 22 April 2020 has put a temporary end to the IP interconnection dispute between Init7, which at the time was primarily active as a backbone ISP, and the Swiss incumbent Swisscom. This dispute began in 2013 and triggered various decisions by the regulatory authority BAKOM/ComCom with the involvement of the Swiss competition authority. This case is described in detail in the BEREC Report of 2017.[116] We refer to this.

---

115 Meier-Hahn (2017).
116 See BEREC (2017), pp. 21ff.

In its ruling of 22 April 2020, the Federal Administrative Court made significant findings and decisions regarding Swisscom's market position on the internet interconnection market. The decision of the Federal Administrative Court, the highest court, has thus determined that Swisscom has (had) a dominant position on the IP interconnection market, at least in the period from 2012 to 2016, which is primarily relevant for the proceedings.

With its decision, the Federal Administrative Court simultaneously annulled ComCom's decision of 27 July 2018, in which ComCom had rejected an access claim by Init7 against Swisscom, arguing that Swisscom had been exposed to sufficient disciplinary forces. It could not have acted independently in the market for IP interconnection. In contrast, the Competition Commission (WEKO), which was consulted as an expert, had found in its expert opinion of 15 December 2014 that Swisscom had a dominant position on the market for IP interconnection. With its (last-instance) ruling, the Federal Administrative Court thus confirmed WEKO's market view.

In terms of content, the Federal Administrative Court made two further significant findings:

(a) IP Transit is not a substitute for peering.
(b) A traffic ratio of inbound and outbound traffic cannot be a price criterion.

The ruling of the Federal Administrative Court has, however, only provisionally put an end to a regulatory procedure which Init7 had initiated on 28 March 2013 by submitting an application to ComCom for an access ruling against Swisscom concerning "interconnect peering".

At the same time as establishing Swisscom's market dominance on the market for IP interconnection, ComCom was obliged to set cost-based prices for peering in terms of Article 11 paragraph 1 of FMG. This determination must be made for the period 2012 to 2016. During this period there was a transit agreement between Swisscom and DTAG which was not customary in the industry and which was detrimental to competition and which was essential for the determination of Swisscom's market dominance. For the period after the termination of the agreement objected to by WEKO, ComCom and WEKO must make current findings on Swisscom's market position on the market for IP interconnection. These procedures have not yet been concluded with decisions at the (provisional) editorial deadline for this study (15.11.2021).

5.2.1.2 Incumbent/Alternate Operator in Serbia

In the context of our survey of NRAs, apart from WEKO on the Init7-Swisscom case explained above, only RATEL in Serbia reported on a regulatory case on IP interconnection. This case concerned a dispute between the incumbent and an alternative operator. The case was resolved by the regulator as part of its market analysis and the incumbent was ordered to offer IP interconnection nationally.

No regulatory authority surveyed has been involved in the resolution of an IP interconnection dispute in the last five years. Furthermore, no case of involvement of competition authorities was reported either (with the exception of the dispute in Switzerland described above).

5.2.1.3 ISPs in Finland

In the interview, Traficom reports on interconnection disputes in Finland in 2014, where large operators also settled their disputes by routing their traffic via Sweden, with corresponding degradations in quality. The regulator advised the operators that they had to inform their customers about the re-routing in advance. Subsequently, there were no more significant disputes. Only smaller operators complained that they did not receive peering.

5.2.2 Disputes between ISPs and CAPs

5.2.2.1 Hetzner/Deutsche Telekom

In Germany, a peering dispute between the hosting provider Hetzner and Deutsche Telekom from 2015 has become known. As a hosting provider, Hetzner provides server hardware, domain and web hosting services as well as cloud products for private and business customers. To make use of its infrastructure and content of their offered services, Hetzner operates public and private peering. The media took an article by Hetzner on its website as an opportunity to report on the paid option of private peering between Hetzner (or customers of Hetzner) and Deutsche Telekom and on the accusation of "double paid traffic" by Hetzner against Deutsche Telekom.[117] Hetzner describes that about two thirds of the network traffic is exchanged via cost-neutral direct peerings, but that routes to some ISPs experience congestion in the evening hours. As a solution to this, Hetzner offered a chargeable upgrade for 5 Euros, which would eliminate these congestions. At the same time, Hetzner referred to net neutrality. Deutsche Telekom commented that a direct network interconnection was possible, but that it did not see any connection to network neutrality. In March 2020, Hetzner published a post on their website[118] stating that they now provide free direct peering with Deutsche Telekom for all customers. Hetzner accuses Deutsche Telekom of seeking payment from both Hetzner and the ISP's customers, contrary to industry-standard cost-neutral peering. Furthermore, Hetzner reports that due to competitive pressure as a result of accessibility problems of its customers, Hetzner is now bearing the costs for direct peering.

---

117 Kuch (2015).
118 Hetzner (2020).

5.2.2.2 Deutsches Forschungsnetz/Deutsche Telekom

During the Corona pandemic, the Deutsches Forschungsnetz (German Research Network) was confronted with increasing data traffic due to increased home work and overloaded transfer points. The upstream service provider of the Deutsches Forschungsnetz was unable to find a short-term solution for the congested network transition with Deutsche Telekom. To improve connectivity, the association turned to another upstream service provider and also offered direct peering to Deutsche Telekom. This proposal was rejected by Deutsche Telekom. As a result, the association commissioned a chargeable "global upstream" with DT.[119] In contrast, the association was able to agree on a fee-free interconnection with the retail ISPs Liberty Global (UnityMedia), 1&1 Versatel, Telefónica Deutschland (O2) and Vodafone Deutschland (incl. Kabel Deutschland).

5.2.2.3 T-Mobile NL Routing

Another spectacular case of turbulence in internet traffic caused by the re-routing decision of a major ISP occurred in the Netherlands in October 2019. Van der Berg (2019) reports the critical situation of mainly small service providers as a result of a sudden change in peering policy by T-Mobile NL. T-Mobile drastically reduced their capacity at the IXP AMS-IX from 200 to 20 Gbit/s in October 2019 and rerouted all traffic of fixed and mobile customers via Germany. In order to reach T-Mobile's customers, all players peering at the AMS-IX had to renegotiate their peering agreements with T-Mobile. The smaller players did not do this and could no longer reach T-Mobile's customers. This also affected a number of cities and municipalities that are directly represented on the AMS-IX. Van der Berg (2019) derives from this situation the requirement that good access with low latency must be guaranteed by large ISPs vis-à-vis small providers. He links this to the demand that, if necessary, even the migration of IXP traffic to private peering must be prevented by regulation. ACM labelled this case an "IP traffic routing incident".[120]

Netflix, Akamai and Google were not affected. T-Mobile had already re-routed mobile traffic before October. This did not lead to any significant deterioration in quality. This changed abruptly when re-routing was extended to the fixed network on 24 October 2019. The performance of many sites collapsed. Packet losses skyrocketed. Some DNS services lost 30% of traffic. The problem resulted mainly from the fact that T-Mobile had not prepared the internet companies for the re-routing. As a result of strong public reactions and pressure from business customers directly connected to AMS-IX, T-Mobile made a quick turnaround after a week and restored the previous connectivity at AMS-IX without any immediate regulatory intervention.

---

119 DFN (2021).
120 ACM (2021), p. 7.

5.2.2.4 Deutsche Telekom / European CDN operator

The Dutch regulator ACM has brought to our attention a dispute that has arisen between DT and a medium-sized European CDN operator. This CDN operator specialises in content delivery for certain services and applications. Due to their traffic characteristics, these applications are characterised by a high quality requirement in transport over the networks to the end customer.

To provide its CDN service, the CDN operator is directly interconnected with a number of backbone operators and ISPs. With others, it maintains transit relationships to reach ISPs' end customers.

In order to gain access to DT's end customers, DT charged a multiple of the market transit price. As an alternative to direct interconnection with DT, this CDN operator had considered transit via backbone providers with which it was itself directly interconnected and which maintained a peering relationship with DT. However, this option was not viable to him, as the capacity utilisation of the network interconnections between DT and the Tier 1 operators was generally 80 to 90% and not between 40 and 50% as is usual in the market. This capacity utilisation was not suitable to accommodate the CDN operator's traffic with a satisfactory quality for him. The operator therefore only had the choice of paying the far excessive price for direct interconnection with DT or foregoing accessibility to DT's end customers which was of sufficient quality for its application.

ACM's conclusion on this situation is the following: The capacity of Tier-1 peering interconnections has been (artificially) scarce in order to prevent the use of (partial) transit over these networks from becoming a substitute for direct interconnection with DT. Transit competition was limited in order to impose excessive prices for direct interconnection. Another implication of this market behaviour are market distortions between medium and larger CAPs/CDNs. Larger operators are obviously able to gain access to some ISPs' networks on more favourable terms than small and medium-sized ones. This further increases their competitive advantages and the network access conditions of some ISPs themselves contribute to increased market concentration in CAPs/CDNs, which they complain about in other contexts.

5.3 Change in the relative power structure of the actors

5.3.1 CDN vs. ISP

The relationship between CDNs and ISPs has changed significantly in recent years. This applies both to vertically integrated in-house CDNs of the large CAPs and to the commercial CDNs. Whereas 10 years ago CDNs exchanged their traffic with ISPs across network boundaries (peering or transit), on-net exchange now predominates, with the CDNs' cache servers collocated directly in the ISPs' network. Only a few ISPs do not allow on-net data exchange and continue to exchange traffic across network borders and POIs. In this respect, the interconnection profile between CDNs and ISPs has changed completely.

Efficient on-net caching requires a series of network planning agreements. In this respect, the relationship between the two groups has become much more cooperative, some even speak of symbiotic.

On-net caching is associated with substantial efficiency benefits and quality improvements. The efficiencies are shared insofar as ISPs regularly bear the costs of hosting the servers and powering them. The CDNs provide and maintain the servers. In terms of network costs, the savings tend to lie with the ISPs. They save core network and possibly also aggregated network costs. In return, they may miss out on earlier transit and peering revenues.

5.3.2 CDN vs. CAP

10 years ago, CAPs still used the services of (commercial) CDNs on a large scale. This has changed fundamentally insofar as the large CAPs have all integrated the value creation stage of the CDNs, i.e. they all operate their own CDN optimised to their respective needs for handling their traffic. In this respect, they have taken the business away from the commercial CDNs - at least to a considerable extent - and now provide these services internally ("insourcing"). At the same time, some CAPs have built up their own external CDN business, especially in the area of cloud services. In this respect, value creation has also shifted towards the CAPs.

These shifts are also reflected in the market capitalisation. Despite the greater market importance of CDNs and the strong growth in business volume, the CDN business remains modest compared to the CAP business. While the CDN market had a market capitalisation of USD 9.24 billion in 2018, it is expected to have a market capitalisation of USD 38.97 billion in 2024.[121] However, this trend can be explained, among other things, by the fact that classic CDN providers are increasingly investing in other business areas and thus positioning themselves more broadly. For example, at Akamai, revenue from the CDN segment ("Edge Technology") in 2021 is down slightly year-on-year (-1%), while the "Security" segment has grown by 25% year-on-year in 2021.[122] In contrast, the market capitalisation of Netflix alone was USD 267 billion and that of Facebook USD 725 billion in November 2021.[123] Therefore, the commercial CDN business is only a small fraction of the business of the big CAPs.

---

121 Altomare (2021). p. 26.
122 Akamai (2021b).
123 OnVista (2021a), OnVista (2021b), retrieved 22.11.2021.

5.3.3 CAPs vs. ISPs

The CAPs' investments in their own backbones and in decentrally localised (on-net) CDNs has permanently changed the classic two-sided market relationship in the relationship between ISPs and CAPs The CAPs now have their own (network) platforms for essential elements of the transport value chain. In the on-net CDN model, (parts of) the network platform are planned and provided cooperatively. The significant investment of CAPs in their own network infrastructure has not changed the ISPs' access monopoly for their end users. However, ISPs and CAPs make joint network planning arrangements in the networks where CAPs operate on-net CDNs. CAPs thus have some influence on the end-user quality of service, even though the ISP remains contractually responsible to the end-user for the quality of service.

One can interpret this shift as a shift of value creation from ISPs to CAPs. At the same time, however, it has also made the relationship between CAPs and ISPs more cooperative in many cases. In these cases, they now decide more jointly on the quality of service delivery.

CAPs now assess their relationship with ISPs as complementary. CAPs such as Netflix rely on ISPs' networks to distribute their video streaming services to end-users. ISPs benefit from this through increased demand for connectivity and growing bandwidth that they can monetise to end-users.[124] In particular, the use of video services, and especially the demand for HD content, is one of the reasons why end customers are demanding faster broadband connections.[125] Furthermore, more powerful networks also inspire new forms of content, which in turn increases the take-up of more powerful networks. This two-way relationship (and dependency), typical of a two-sided market, initially supports a cooperative model of dealing with each other. However, it can also be the cause of disputes when the equilibrium of the parties is disturbed or a new equilibrium is sought. Such a disturbance of the equilibrium can occur, for example, if a "settlement-free" relationship is to be transformed into one in which one side would have to make payments to the other.

This rather growing complementarity of the relationship between ISPs and CAPs contrasts with the very antagonistic relationship that was still expressed in the interconnection dispute between Netflix and Comcast and Verizon. Corresponding effects could be observed in particular in 2013/2014 in this dispute in the USA. Already at that time, Netflix accounted for 34.89% of the incoming traffic at peak times in the American fixed network.[126] This continuing trend necessitated regular capacity expansions of peering handover points between the network operators handing over Netflix traffic to the retail ISPs Comcast and Verizon. In addition, Netflix moved its traffic

124 Netflix (2021), for example, argued emphatically.
125 As shown in Figure 1-7.
126 Sandvine (2014).

from the CDNs it had previously used, some of which were in paid peering relationships with these ISPs, over its own CDN infrastructure to providers that already had peering agreements on bill-and-keep terms with these ISPs. This initially allowed Netflix to reduce its costs significantly. Due to the growing asymmetry in these formerly balanced connections and the simultaneous loss of paid peering revenues, the ISPs decided not to further expand capacity at the exchange points in question. As a result, over time, there were increasingly frequent bottlenecks and unsatisfactory accessibility of the streaming offer for paying Netflix subscribers at the ISPs concerned. This conflict was at the expense of consumers at the time, as Netflix and the respective ISPs accused each other of being responsible for the situation. Ultimately, however, Netflix was able to reach an agreement with these ISPs on direct paid peering. This agreement subsequently also restored the usual quality of service for end customers.

In this context, however, it is questionable whether smaller CAPs, whose share of traffic at peak times is relatively small, could also be affected by comparable restrictions. Furthermore, it is also questionable whether smaller CAPs in this situation would even be able to negotiate comparable conditions as Netflix with large ISPs in a similar time horizon. Commercial CDNs are thus attractive intermediating business partners for smaller CAPs, as they not only reduce technical hurdles and ensure high quality in the delivery of online content, but at the same time have greater negotiating power vis-à-vis large ISPs.

CAPs that feed their traffic relatively "locally" into the ISPs' networks via on-net CDNs claim to generate a number of benefits for the ISPs:[127] First, they save or avoid transit fees they would have to pay if they had to take traffic less locally or even far away and using international backbone capacity. Second, if an ISP uses multiple OCAs, it saves on its own core network costs. The traffic is taken over by a server (relatively) close to the customer and does not have to be routed via the ISP's core network. Third, network resources are saved by updating the content servers during off-peak hours. Fourth, in addition to these direct cost benefits, there are advantages for the ISP as a result of the better quality arriving at the end customer. The willingness of customers to switch is reduced. Fifth, ISPs have full control over their network. They can determine and optimise the locations of the cache servers based on their customer structure, network capacity and load structure of the network.

There is speculation in the literature that CAPs could also integrate into the ISP level as a result of their advancement in the value chain. Dey and Yuksel (2019), for instance, expect this direction of integration and see the avoidance of paid peering as a motive. Furthermore, they see CAPs dominating in market capitalisation and having approximately the same footprint as ISPs. They refer to the newly emerging entities as "sugarcane ISPs". Sugarcane ISPs would be geographically closer than ISPs today and

127 As Netflix (2021a), pp. 23ff argued.

would have less incentive for peering. They also expect the resulting incentives to hinder (content) competitors in order to increase their own demand.

We think this scenario is unlikely. CAPs would invest in a regulated business. This is not in line with their business policy principle. Moreover, they would expose themselves to strong criticism of (potentially) violating net neutrality. They have constantly and intensively struggled for this principle. They would thereby lose their credibility and expose themselves to the risk of comprehensive regulation of their entire business.

Nevertheless, there are investments by CAPs in access networks. However, these focus on improving connectivity in developing countries. For example, Google and Facebook have developed their own Wi-Fi initiatives to build public Wi-Fi hotspots.[128] Such investments can be found in countries such as India, Indonesia, Thailand and Nigeria.

In reality, many more ISPs are now integrated in the content and online business than CAPs in the ISP business. This is strikingly true for all cable network operators who are active in the TV and VoD business. But it also applies to the (large) telcos. They are often active with their own platform in TV and VoD, but also in content and broadcasting rights business.

5.3.4 Cloud provider vs. ISP

The cloud business has developed particularly dynamically in the last five years. The large cloud providers offer cloud services not only to business customers, but also to large CAPs such as Netflix, Apple and Spotify. They are responsible for significant parts of the IP traffic. They largely rely on their own backbones and only request limited transit services from backbone ISPs. In terms of services for business customers, they are in direct competition with ISPs. They have a regional and local presence on the network side via CDN configurations and are also directly present in the ISPs' networks in on-net configurations.

The public cloud market is dominated by Amazon, Google, IBM and Microsoft. Table 5-1 shows the global market shares of the most important providers in the Infrastructure as a Service (IaaS) segment. The European cloud market is also relatively highly concentrated. Especially in the IaaS and PaaS (Platform as a Service) segments, the market is dominated by American cloud providers, as Figure 5-1 shows. However, compared to the global market, two European telecommunications companies are also represented among the top 6 providers in Europe with Deutsche Telekom (2%) and OVH (4%).

128 Abecassis et al. (2018). S. 46.

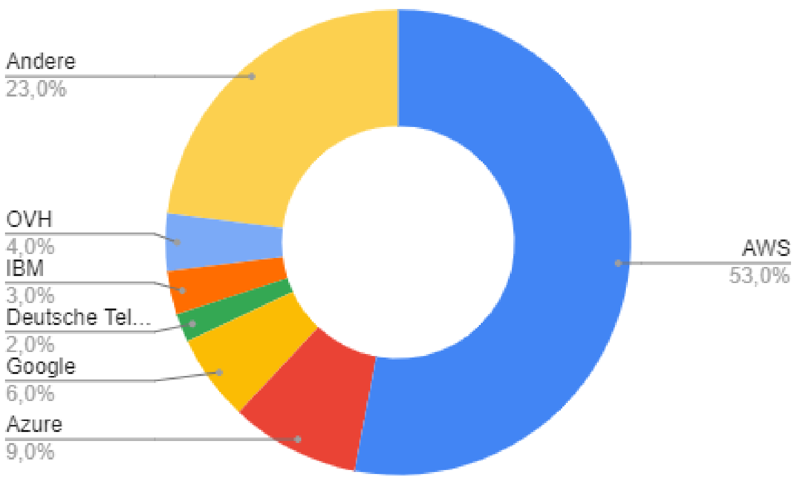
The large cloud providers have to some extent overtaken the backbone ISPs as the backbone of the internet.[129] Through their networked infrastructure, they have contributed significantly to the meshing and flatter hierarchy of the internet.

Table 5-1: Global IaaS Public Cloud Services Market Shares 2019-2020 (USD Million)

Company	2020 Turnover	2020 Market share (%)	2019 Turnover	2019 Market share (%)	2019-2020 Growth (%)
Amazon	26.201	40,8	20.365	44,6	28,7
Microsoft	12.658	19,7	7.950	17,4	59,2
Alibaba	6.117	9,5	4.004	8,8	52,8
Google	3.932	6,1	2.367	5,2	66,1
Huawei	2.672	4,2	882	1,9	202,8
Other	12.706	19,8	10.115	22,1	25,6
Total	**64.286**	**100,0**	**45.684**	**100,0**	**40,7**

Source: Rimol (2021), Gartner (2021).

Figure 5-1: Market shares IaaS, PaaS and hosted private cloud services in Europe (2020)



Source: WIK-Consult based on KPMG (2021).

They can substantially bypass the Tier 1 ISPs with their own networks and are highly independent of them, as we have shown in Section 3.2.3. This increasing interconnectivity of a few large networks has contributed to the downward trend in the transit revenues of the Tier 1 operators. The large cloud providers have taken over from the backbone operators as the central transport providers of the internet.

129 Arnold et al. (2020).

6 Implications for Europe's digital sovereignty

6.1 Introduction

In recent years, a trend towards more "strategic autonomy" has emerged among policy makers in the major global economic blocs (US, Asia and Europe). Countries are increasingly reviewing their resilience to and dependence on foreign suppliers of critical services and products, especially from countries outside their respective economic blocs.

In terms of key ICT infrastructures, this strategic autonomy is often referred to as 'digital sovereignty'. This topic ranges from debates on 5G hardware providers to initiatives related to cybersecurity and European data infrastructures such as GAIA-X, but also includes strategic investments in artificial intelligence, robotics and high-performance computing. The goal of digital sovereignty is to strengthen Europe's research and industrial capacities, as these technologies are considered key factors for future innovation and economic growth.

However, a European benchmark by WIK-Consult from 2020 showed that digital sovereignty is not based on a uniform definition. Policy makers attribute different tasks and goals to it and use different terms, e.g. technology sovereignty or strategic autonomy.[130] Despite different interpretations, the authors of this benchmark were able to identify three common dimensions of digital sovereignty: 1) (private) data protection, 2) cybersecurity and 3) strategic interests. The privacy dimension is about the ability of individuals to control their digital lives and data. The cybersecurity and strategic dimensions of digital sovereignty refer primarily to actions at the collective level of countries and the EU to (re)gain control and leadership in the digital domain.

After the detailed description and analysis of the trends in the IP peering and transit markets, this chapter focuses on the implications for Europe's digital sovereignty with regard to the following groups of players:

- European content and application providers;
- European providers in the areas of transit, peering, CDN, IXP; and
- European end users.

6.2 Digital sovereignty at a glance

Before discussing specific implications for digital sovereignty from the developments described in the IP peering and transit markets, we would like to highlight two aspects that are relevant for classifying digital sovereignty in the context of interconnection markets.

130 WIK-Consult (2020).

Digital sovereignty is about finding a balance

As we have already noted in our 2020 European benchmark on digital sovereignty,[131] there is a fundamental tension between the concept of the internet and digitalisation, which enables data sharing without geographical boundaries, and the concept of sovereignty, which refers to a specific geographical area. Moreover, most of the policies of the European countries studied seem to underline that neither digital sovereignty nor strategic autonomy lead to autarky or protectionism. Rather, digital sovereignty is about finding a balance between achieving one's autonomy and maintaining a diversified portfolio of providers and international trade relations, which are important for many EU economies.

In this context, the BMWi (2021) refers to Draghi (2019), while stating a similar position; "... ein Staat bzw. ein Akteur [kann] auch bei unvollständiger Unabhängigkeit souverän sein. So geht es im Kontext der Souveränität immer auch um ein Abwägen, ein „Abhängigkeitsmanagement“, und die bewusste Entscheidung für oder gegen etwas sowie die kontinuierliche Neubewertung gegenwärtiger Abhängigkeitsbeziehungen.“ *[...a state or an actor can be sovereign even with incomplete independence. In the context of sovereignty, then, it is always about trade-offs, about dependency management and the conscious decision for or against something, as well as the continuous reassessment of existing dependency relationships*]. With reference to Kagermann et al. (2021), BMWi concludes that digital sovereignty should rather be understood as "...die Möglichkeit mehr Unabhängigkeit zu erzielen, wo sie erwünscht ist, z. B. in Bereichen, die die nationale Sicherheit und den Schutz von Wirtschafts- und Personendaten betreffen (Kagermann et al. 2021)..." *[...the possibility of independence where it is desired, e.g. in areas concerning national security and the protection of economic and personal data...*].

Conflict of norms between digital sovereignty and internet governance regimes

Ten Oever (2021) points out that there might be conflicts of norms between private internet governance (based on multi-stakeholder self-regulation) and increasing rule-making through state interference since the 2010s. The author concludes that these two regimes should not be understood as opposing forces, but rather as two different parts of the internet governance regime. However, there are different emphases; the private Internet focuses more on creating interoperability and interconnection through coordination and standards development. The multilateral state regimes tend to prioritise a different set of goals (including sovereignty, economic prosperity, limiting harmful content and national norms and values), rather than interconnection and interoperability.

131 WIK-Consult (2020).

The author gives several examples, including "Schengen routing", which aims to keep traffic originating from and destined for a particular country or group of countries within the geographical boundaries of that country or area. However, this is contrary to the dynamic routing of traffic, which can be seen as an essential design feature of the Internet.[132] Ten Oever also notes that several states want to extend their influence over ICANN's decision-making on the use of top-level domains and IP addresses. [133] Other states, such as Russia and China, have gone even further, enacting national regulations and creating their own internet infrastructures to better control the internet.

Mueller (2017) also argues that there is a mismatch between Internet governance and national sovereignty, as the former aims to create a global Internet while the latter reflects a regime in which nations seek to apply rules based on their own territorial reach. Budnitsky (2017) describes the essence of Mueller's book as “...supporters of the global Internet should be principally concerned about ... state sovereigns’ efforts to align global communications along the borders of national jurisdictions.” To preserve the benefits of digital globalisation, he even recommends that supporters of the Internet's emancipatory promise establish a transnational virtual nation committed to the principles of borderless communication and take global Internet governance into their own hands.

Hellberg (2019), in another article on internet routing and the implications for digital sovereignty, writes that "governments should have a better understanding of the nuances of data routing around the world, including the realization that internet cabling and routing does not allow for geopolitical distinction." and that there is a need for those who make laws and regulations to "... need to collaborate with those that design and implement how the internet works in their respective countries".

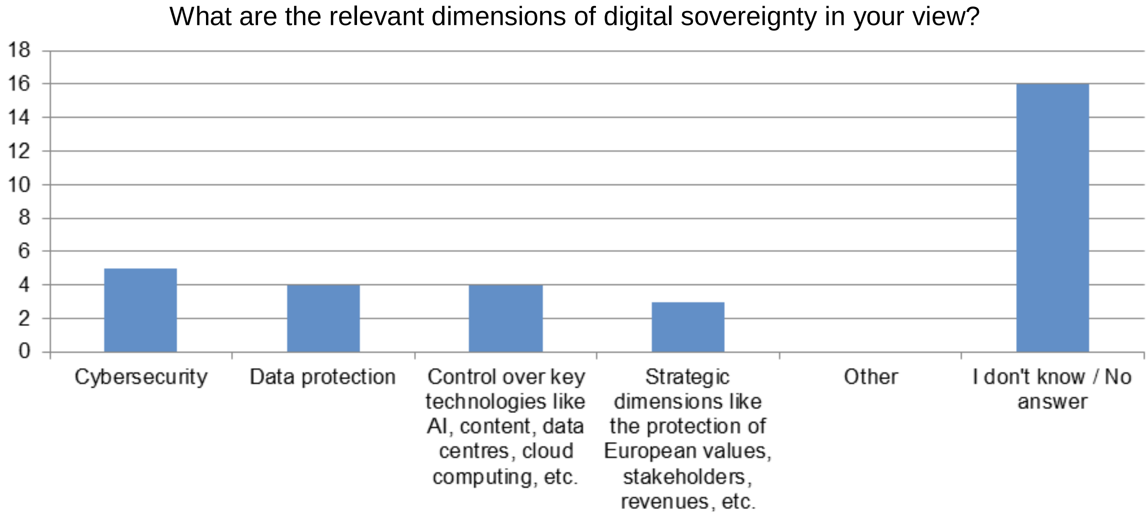
6.3 Findings on digital sovereignty from the IRG member survey and interviews

In our survey on IP peering and transit among European NRAs, we also asked for their opinion on the relevant dimensions of digital sovereignty. Of the 22 respondents, only 5 (BG, CZ, PO, RO, RS) confirmed that aspects such as cybersecurity, data protection, control over key technologies and strategic aspects are relevant dimensions of digital sovereignty. However, the majority (16) had either not provided any information or did not know whether these aspects are relevant to digital sovereignty.

132 The forwarding of data packets over the Internet is carried out by routers that use the prefixes of the destination IP addresses to dynamically determine which is the shortest and fastest path to the final destinations and then forward the packets to the next routers, which repeat this process until the packets have reached their final destination. See also Section 6.5.1. National jurisdictions are likely to play a subordinate role here. The routing agreements between delimited autonomous systems are likely to be much more relevant.

133 Internet Corporation for Assigned Names and Numbers.

Figure 6-1: Dimensions of digital sovereignty considered by the European NRAs



Source: WIK-Consult.

Based on this question, we wanted to know if the NRAs see any problems in the transit and peering markets in the context of digital sovereignty, and received only one positive answer from the Serbian NRA, but also two clear negative answers from the NRAs of Bulgaria and Spain. All other 7 responding NRAs did not know (CH, CZ, FR, IR, NL, PO and RO).

These answers give rise to the assumption that digital sovereignty in relation to IP peering and transit has a subordinate role on the NRAs' agenda, at least for the time being. Accordingly, NRAs have not considered any measures related to digital sovereignty that should be considered at the European level (including Schengen routing[134]).

In the nine interviews we conducted with IP peering and transit market players, four of them commented on digital sovereignty (DE-CIX, Facebook, Google and the Finnish NRA Traficom). Below we have summarised their observations and will return to specific aspects in the following sections:

- **DE-CIX,** operator of an IXP, underlined the increasing importance of cyber security and stressed that it is important to ensure that not only specialists know how the internet works. However, there is a tension between cybersecurity and dependency, as cybersecurity services can result in greater dependency on the companies providing them. In terms of public services, this may therefore have implications for digital sovereignty. Last but not least, it was noted that the main

134 The data will only be forwarded within the European borders, see also Section 6.5.1.

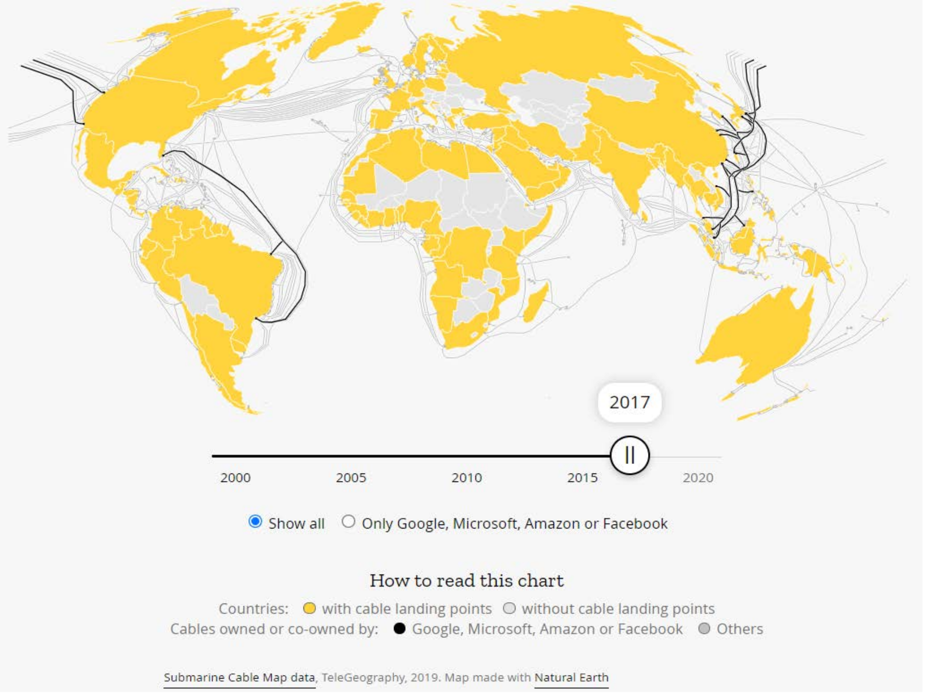
focus of regulation, if any, should be on ensuring an open and neutral internet to avoid artificial bottlenecks and privatisation of the internet by some very large parties. To this end, it would be good for NRAs to monitor prices in the IP transit and peering markets.

- **Facebook** does not see any issues with transit and peering in the context of digital sovereignty. Facebook's understanding of digital sovereignty focuses on ensuring that certain data is stored within Europe or the respective Member State. The inclusion of aspects such as cyber security and strategic issues (e.g. network components used for interconnection) is considered to be too broad.
- **Google** considers digital sovereignty relevant, but it should be taken into account that it does not drive competition in the IP wholesale market, which ultimately promotes the efficient exchange of traffic and thus a profitable business. Furthermore, Google does not consider requirements on region-specific cloud services as digital sovereignty, but rather as a legal issue to encourage providers to process the collected data locally. However, from a security perspective, this (local) solution is no better than keeping data outside the country. Moreover, this "local data processing requirement" might even act as a barrier to entry for small cloud providers, as these requirements imply that local data centres become necessary in the context of geographical-diversified scope of business.
- **Traficom** believes that digital sovereignty is about having key resources under one's own control (e.g. control over domain names). This includes an obligation for ISPs to keep certain key functions in Finland in order to ensure the functioning of the networks in Finland. In addition, for reasons of data protection, it is mandatory that content remains in Finland. If data leaves the country due to re-routing, ISPs are obliged to inform their end customers. Traficom has developed "guidelines" which, in addition to the above-mentioned aspects, also concern network security, good connectivity through submarine cables and Europe's role in setting global standards (in opposition to the USA/Asia).

6.4 Implications for European content and application providers

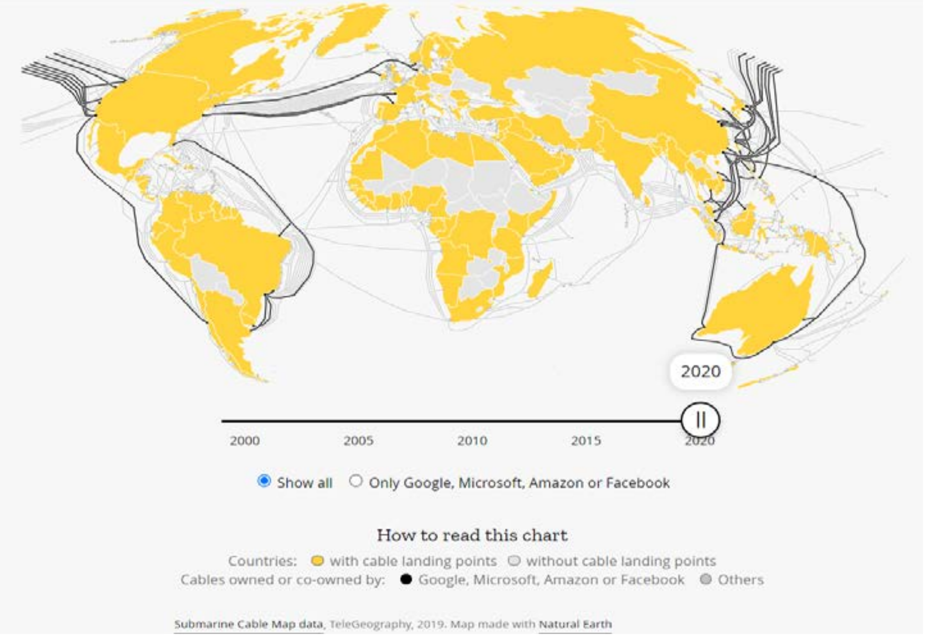
As described in Section 1.2, the number of IXPs and volume of traffic exchanged via IXPs have continued to grow as expected, with traffic exchanged via bilateral private peering agreements increasing relatively at the expense of multilateral peering via IXPs. This explicitly applies to the large (non-European) CAPs, which are pursuing vertical integration strategies and have significantly expanded their submarine cable capacities between the US and Europe and with Asia between 2017 and 2020 (see Figure 6-2 and Figure 6-3). They have also established data centres in Europe and integrated CDN networks into their operations. In most cases, they have also managed to convince European ISPs to host on-net cache servers on their networks.

Figure 6-2: Submarine cable map data 2017



Source: Submarine Cable Map 2019, TeleGeography.

Figure 6-3: Submarine cable map data 2020



Source: Submarine Cable Map 2019, TeleGeography.

Cost advantages for vertically integrated CAPs

The implications for European CAPs are that they have to compete in Europe with mainly US-based CAPs, which have minimised their previous geographical cost disadvantage by buying transport capacity via submarine cables (instead of relying on backbone providers for transit) and storing more content in European data centres. At the same time, US-based CAPs further benefit from scale-based cost advantages by integrating CDNs rather than relying on third-party CDN offerings.[135] In addition, US-based CAPs can fine-tune their cache servers on European ISP networks to maximise the quality and performance of their end services.

European CAPs using third party CDN services may therefore be at a cost disadvantage and below a certain size may not be able to convince ISPs to allow the placement of cache servers on their access networks. However, it is not clear whether placing cache servers at the edge of ISPs' networks will in all cases result in significantly poorer quality for end users.[136] The number of handover points and the volume of traffic play an additional role here.

Competition concerns as a result of the vertical integration of CAPs

Song notes that there is not only a shift of ownership of submarine cables from telecom providers to large CAPs such as Google and Facebook, but also to nation states as part of a geopolitical cyber strategy.[137] Song points to three relevant aspects in this regard:

- Submarine cables effectively become a private network connecting CAPs' data centres. According to Song, companies like Google are keen not to act as telecoms and have therefore publicly stated that they will not resell capacity on their cables.
- However, large CAPs could swap capacity with other companies that have capacity of a comparable size. This could result in large parts of submarine cable capacity only being accessible to other CAPs with similar investments.
- Nations, first and foremost China, are pursuing similar strategies (vertical integration) and investing considerable sums in the development of a geographically strategic infrastructure. The goal seems to be that internet data can flow entirely around the world via a fibre-optic infrastructure owned by China.[138] China's increasing outward expansion and investment in

135 In one of the interviews, a factor of 40 was mentioned as the cost difference between buying a third-party CDN and owning one.
136 Netflix in Germany, for example, has (for other reasons) placed its cache servers at the edge of the DT network at regional delivery points, without any significant impact on quality for end users.
137 Song (2019).
138 The author mentions the SAIL cable connecting Africa to South America, the PEACE cable connecting Asia to Africa, and a possible trans-Pacific initiative connecting China directly to South America.

> communications infrastructure development overlaps geographically with many initiatives under the Belt and Road strategy, which aims to strengthen China's economic ties with 71 countries by investing in roads and waterways. Song believes that by embedding surveillance or even censorship functions in the (digital) infrastructure, these expansive strategies could compromise democracy and national sovereignty.

ACM (2021) notes in its market analysis[139] that due to the vertical integration of non-EU CAPs, it may be necessary and desirable in certain cases to attach conditions to proposed acquisitions in order to avoid restrictions of competition. According to the ACM, this applies to providers and customers in IP interconnection, for example CAPs, ISPs and IXPs. When these parties merge, it may be necessary to impose IP interconnection obligations on the newly merged entity, for example to ensure that there are sufficient opportunities for third parties to interconnect on reasonable terms.

ACM also referred in its 2021 market analysis to an assessment by the European Commission (EC) of Liberty Global's proposed merger with Vodafone in the Netherlands.[140] The EC concluded, among other things, that Liberty Global was in a position to obstruct the distribution of competing (OTT) providers' content through its position on IP interconnection. One of the key aspects was a contractual clause that high-quality interconnection through peering would only be offered on the condition of exclusivity of content and otherwise peering would be refused. Therefore, the Commission found that Liberty Global's interconnection policy could (at least in theory) prevent competing OTT providers from reaching Ziggo's end customers, or at least prevent them from reaching Ziggo's end customers with competitive quality due to congestion. To avoid the potential problems identified, Liberty Global has committed to maintain at least three congestion-free routes to Vodafone-Ziggo's IP network.[141]

As mentioned above, Dey and Yuksel (2019) assume that CAPs could also vertically integrate with ISPs due to their rise in the value chain and to avoid paid peering. They refer to the integrated CAP/ISP entities as "sugarcane ISPs" and expect that they would have fewer incentives to peer and incentives to hinder (content) competitors in order to increase demand for their own services. However, we consider this scenario unlikely, as CAPs would invest in a regulated business, which tends to run counter to their business policy principle of avoiding regulation. The avoidance of such businesses can already be observed in the limitation to exclusively use their own submarine cable capacity.

139 Section 4.4.1 of ACM (2021).
140 European Commission (2018).
141 See chapter 4.5 for further description and sources.

6.5 Impact on European providers in the areas of transit, peering, CDNs and IXPs

Much of the internet traffic is handled by the large CAPs, which have integrated their own CDN and can thus deliver almost all their traffic locally to end users. As a result, transit traffic via traditional (European) Tier 1 telecoms has declined sharply. In addition, the large CAPs have moved to offer free private peering instead of public peering via IXPs, reducing the importance of public peering at IXPs.

In the following sections, further relevant details for the individual parties are explained in more detail.

6.5.1 Impact on European transit service providers

Transit as an alternative

In particular, the traditional Tier 1 providers have lost their significant role on the Internet as providers of the general backbone infrastructure. It also emerged from the interview with Deutsche Telekom that large CAPs and cloud providers from the USA, but also from Asia, increasingly control the international backbone infrastructure and the traditional telecom companies have become smaller players. As a result, more and more internet traffic in Europe is routed through private networks of large non-European market players (including their own submarine cables, connections and data centres in Europe), up to on-net cache servers in the networks of European ISPs.

The remaining transit business seems to be concentrated mainly in those areas where European Tier 1 providers also take on the role of an end-user ISP. One of the things that emerges from our discussions is that there are indications that the ongoing price erosion in the IP transit market could lead to a reduction of investments or even market exit. However, the transit market is an important (back-up) way to ensure resilience of European networks and a last resort to reach end-users and provide end-to-end connectivity.

Encryption versus Schengen routing

The strong forward integration of large (mostly US) market players requires consideration of another aspect of digital sovereignty: the possible violation of European data protection and privacy policies, sometimes by foreign intelligence services, if traffic originating in and destined for Europe is routed via non-European countries. After several breaches in this context, a debate began in 2015 on so-called "Schengen routing", which proposed limiting the routing of data between European member states to autonomous systems located in Schengen countries.

Pohlmann et al. (2015) simulated a virtual "Schengen network" in a scientific study. The authors concluded that this could lead to an unequal distribution of economic disadvantages between the EU countries, which would further increase the inequalities between the countries of the EU internet market.[142] Dönni et al. (2015) conducted measurements to quantify compliance with Schengen routing on the internet today and came to similar conclusions: Overall, 35% to 40% of routes (in over 1100 different ASes in the Schengen area) are 'Schengen compliant', with compliance levels varying widely between 0% and 80% depending on the country.

Pohlmann et al. (2015) further investigated an alternative to Schengen routing, namely data encryption through two technologies (IPSec and SSL/TLS[143]), and concluded that the security (of Schengen routing) depends entirely on the policies and constraints of the routes, but neither the content nor the physical communication layer is protected. The authors therefore concluded that switching to encryption of traffic seems to be the most sensible approach, rather than simple (routing) measures that risk technologically isolating Europe. Since foreign intelligence services can also systematically collect a large part of telephone and internet connection data in Germany and store it in the home country,[144] it is doubtful whether restricting European data traffic to the Schengen area would prove expedient.

More recently, Hellman (2019) also points out that governments should be aware that "... it will be nearly impossible to implement true data localisation, so truly private information will have to be encrypted in some form." However, the author also stresses the importance of rigorous monitoring of network routes (by NRAs), as this helps to quickly identify if data is being routed - accidentally or maliciously - to places it was not intended, which can have serious repercussions.

Network equipment that could pose a threat to national security

Finally, there is the question of control over the equipment installed in the European peering and transit networks. These are, on the one hand, the on-net cache servers of the large CAPs and, on the other hand, the general problem of network control and routing equipment whose manufacturers are not based in Europe.

From our interviews and the information gathered about Netflix's CDN concept, it is not clear how transparently the Open Connect servers function in the ISPs' networks and

142 Belgium, Spain and France are among the countries most affected economically, as a large number of the available routes in these countries are handled by autonomous systems outside the respective country. The authors also assume that the effort required to implement mandatory Schengen routing could even lead to higher prices for some market segments and (internet) services.

143 Internet Protocol Security (IPsec) is a protocol suite designed to enable secure communication over potentially insecure IP networks such as the Internet. The aim is to provide encryption-based security at the network level. Transport Layer Security (TLS), also known by its predecessor Secure Sockets Layer (SSL), is an encryption protocol for secure data transmission over the Internet that includes TLS Handshake, which involves secure key exchange and authentication.

144 Poitras et al. (2013).

whether this poses a threat to the digital sovereignty of these networks. However, it is clear from the interviews that the cache servers may not be opened by the ISP, although ownership has been transferred to the ISP. Netflix, however, pointed out that its "black box" is not technically secretive inasmuch as it is based on open source software (e.g. Linux/FreeBSD) and the ISP has control over e.g. the update period of the cache and physical access to it. Apart from DT, we are not aware of any other ISPs that have expressed concerns in this direction.

From the interview with Google, it emerged that the choice of equipment provider currently still depends on cost, availability and scalability, but that digital sovereignty could become more important in the future. Init7 told us that an evaluation of providers has taken place in Switzerland in 2020. However, many market participants using Huawei stated that avoiding certain providers is difficult and that (wholesale) customers do not see this as critical.

WIK-Consult (2020) examined the specific policies in Europe with regard to digital sovereignty and found that the focus is on mobile networks and in particular the new 5G networks. Here, the measures taken in countries vary and seem to be guided by existing economic and geopolitical alliances. However, the cost of removing equipment from certain providers on existing (mobile) networks should not be underestimated. Recently, the FCC in the US released the projected costs of its Supply Chain Reimbursement Program, which was introduced in the wake of security concerns as operators are currently rolling out their 5G networks primarily with equipment from Chinese companies such as Huawei. The FCC received requests for reimbursement based on operators' plans to replace affected hardware on their networks. The expected cost is USD 5.6 billion compared to the expected USD 1.8 billion, a threefold increase.[145]

6.5.2 Implications for European peering parties

Market concentration and justification of the option to publicly assess IXPs

We note that the number of IXPs has almost doubled in the last 10 years.[146] The growing geographic coverage of these exchange points for internet traffic has also facilitated the growth of peering at the expense of transit. However, it is mainly bilateral (private) peering of traffic via IXPs that has increased at the expense of multilateral (public) peering operated by the major CAPs; 10 to 15 years ago, more than 50% of CAP traffic was carried via IXPs, whereas today it is less than 10%.

Apart from the strong concentration in the (European) peering markets, which leads to the larger parties exchanging traffic via (private) peering, the smaller peering parties still

145 Mitchell (2022).
146 87.5%, from 136 in 2017 to 255 in 2020, Euro-IX (2020), p. 6.

need the option to perform public peering at IXPs. In terms of digital sovereignty, it seems important here to ensure that the market behaviour of the large (US) CAPs does not interfere with the possibility for smaller (European) market players to conduct public peering at European IXPs. This was confirmed by Google in our interview, which highlighted the importance of public peering at IXPs for new players due to the low entry barriers and the fact that IXPs can be considered as complete ecosystems.

Restrictive peering policies are not synonymous with digital sovereignty

Peering policies make transparent, among other things, a company's conditions for settlement-free peering. As described in Section 2.4.1, these policies have more to do with the required number of peering sites, the minimum volume of traffic exchanged and the ratio of inbound to outbound traffic. A restrictive or selective peering policy therefore has nothing to do with digital sovereignty, but rather seems to serve to protect the traditional (transit) business of Tier 1 parties in areas where they are also ISPs. In fact, most US-based CAPs and peering partners have quite open peering policies (with only limited terms for largely settlement-free peering arrangements) and are present at many IXPs.

6.5.3 Implications for European CDN providers

Merging cloud and CDN markets

Due to economies of scale, large CAPs and cloud providers have been able to pay for CDNs that allow them to serve their end customers locally with their content and thus in better quality. There are also cost benefits as transport costs are reduced. Since these large companies can also sell CDN services on a commercial basis, they most likely have a cost advantage over European CDNs. Therefore, other aspects or additional functionalities become important for European CDN providers to remain competitive.

As was evident from our interviews, none of the former Tier 1 operators were successful in building a CDN business. One of the predictions is therefore that the classic CDN market will continue to shrink until it integrates with the cloud market, which is driven by synergies in the offerings of large providers such as Google and Amazon Web Services (AWS). In addition, cybersecurity as a service has become a selling point for CDN providers. An example of this is Akamai's CDN services, whose strongest selling point is DDoS defence.

The digital sovereignty aspect here could be that European end-users, businesses and governments could become dependent on several large (US-based) cloud/CDN providers. This is also true in terms of security, unless European CDN operators can consolidate their market position through unique selling points and added values of their offering.

The counter-arguments from our discussions with CAPs are that no personal data would be processed by the CAPs' cache servers and that there would be no government control of the (US) CAPs. Therefore, the link between CDNs and digital sovereignty is more of a political issue than a regulatory one, as recently highlighted in South Korea. Netflix faces the challenge of serving South Korean end-users with cache servers from abroad due to a legal change.[147]

6.5.4 Impact on European IXPs

As described earlier, the role of IXPs has changed; the IXP operator DE-CIX noted in our interview that it has evolved from the "spider in the web" to an important backup in case of unexpected congestion of private peering connections. This was confirmed in discussions with large CAPs, where only a very small part of the traffic flows over IXPs, but which nevertheless stated that they need this connection as a fallback option in case of bilateral problems and for accessibility for smaller market participants ("catch-all"). In addition, multilateral public peering connections at IXPs remain crucial as they allow smaller market participants to exchange all their traffic at a single point. Furthermore, IXPs have developed complementary services such as hosting and providing direct connectivity for cloud providers, but also direct connections to the internet for larger companies. This was evident in our interview with Google, where IXPs were described as complete ecosystems.

According to DE-CIX, the infrastructure for internet connections should be based on open (regulated) wholesale access in Europe with a nationwide fibre roll-out to prevent artificial bottlenecks and the privatisation of the internet by a few very large parties.

In terms of digital sovereignty, DE-CIX also noted that there is an increasing focus on cybersecurity. This leads to an increased importance on the security of the IXP's own infrastructure and resulting in stricter requirements for the internal organisation, but also towards external providers. In this context, Hellberg (2019) notes in her recommendation on cyber regulation that "it is important to ensure that organisations engage directly with cloud providers to promote transparency in data transfer."

DE-CIX also sees what happens to the data, and where it is forwarded to, as being relevant. Therefore, it is advantageous if the data centres are located in Europe or in an EU country. For DE-CIX, this explains why Frankfurt, the place where DE-CIX set up its first IXP, is still a popular location for a data centre.

The Dutch regulator ACM also noted in its 2021 market report on the IP interconnection market that there is a concentration of IXPs in Amsterdam, which makes the region attractive for many players in the digital ecosystem. However, ACM also warns against

---

147 See also Chapter 2.2.1.

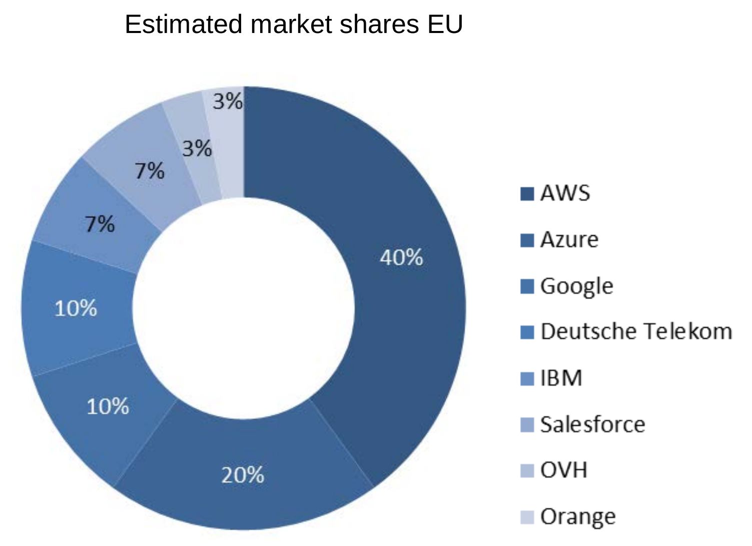
too much centralisation of IXP infrastructure, as this poses a risk to resilience. In case of an incident in this region, many services could be affected. Therefore, the 'Ministry of the Interior and Kingdom Relations' is working on the geographical diversification of data centres in the Netherlands.[148]

6.6 Impact on European cloud providers

Focus on US players

The European cloud market has grown steadily, from €1.9 billion in 2017 to €7.3 billion in Q2 2021, but it has also seen a strong concentration of non-EU players: AWS, Azure, Google and Salesforce have an aggregated market share of 77% in 2021. The importance of this market globally is also demonstrated by the growth of Alibaba, the dominant cloud provider in China, from USD 4 billion in 2019 to more than USD 9 billion in revenue in 2021. Huawei, the provider, has also made a hard reversal: away from selling devices and towards investing heavily in its cloud services business.[149]

Figure 6-4: Estimated market shares in the European cloud market 2021



Source: WIK-Consult based on available market data, September 2021.

European companies such as DT, Orange and OVH have only a small market share (16%).

148 https://www.denationaleomgevingsvisie.nl/samenwerking+and+implementation/programmes/spatial+strategy+datacenters/default.aspx
149 Statista 2022.

In our interview, DT confirmed the dominance of the large cloud providers, which are offering more and more services, and expects a takeover of the CDN markets by cloud providers, as these services are realised in a technically comparable way. DE-CIX noted that AWS, Microsoft and probably Cloudflare also have a very dominant market position in terms of cybersecurity solutions.

In relation to digital sovereignty, the following observations can be made:

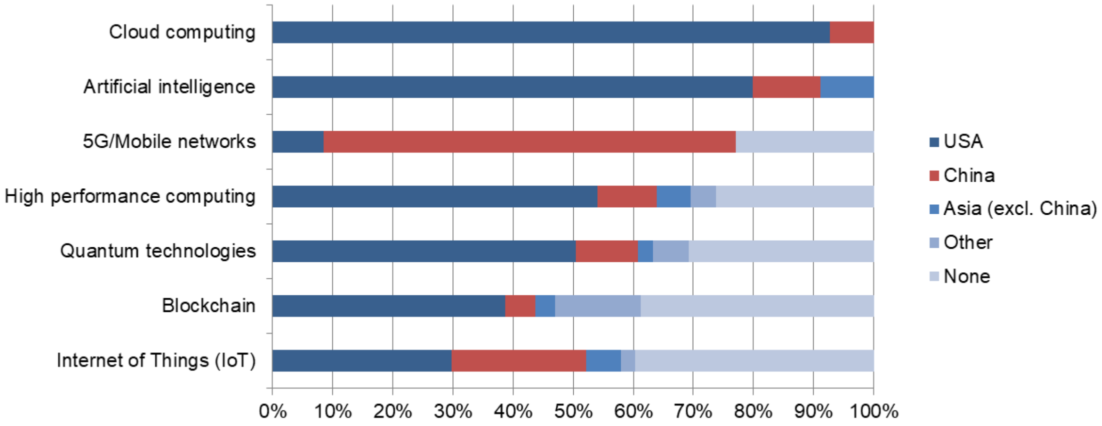
- Deutsche Telekom, as the largest European provider, established its own cloud business with the Chinese provider Huawei in 2016, but now also acts as a reseller for cloud services from AWS and Microsoft.[150]
- While cloud providers used to require transit operators to reach all networks, research shows that they can now reach more than 76% of all autonomous systems without the backbone networks of Tier 1 and Tier 2 providers.[151]
- As with data centres, geography can be an important aspect as it influences over which routes data should be sent. However, the cloud providers themselves state that local solutions offer no advantages over data outside the country from a security point of view. Nevertheless, Google operates special cloud services for the German market and has a partnership with Deutsche Telekom for a "sovereign" cloud service.

These aspects can be further illustrated by the following three figures, which show that Europe is heavily dependent on US cloud computing, among other things (Figure 6-5). Figure 6-6 shows that worldwide, data sovereignty plays an important role (53%) or is even a must (24%) for companies opting for cloud solutions. Figure 6-7 shows, however, that despite all efforts in 2021, 37% of the experts surveyed worldwide still have concerns about data sovereignty, data residency and data control.

150 Comment: Europe's cloud providers lack courage vis-à-vis their US rivals. https://www.handelsblatt.com/meinung/kommentare/kommentar-europas-cloudanbietern-fehlt-gegenueber-den-us-rivalen-der-mut/26962646.html. Accessed 10 February 2022.

151 Arnold et al. (2020); Google could reach 174 AS networks without transit providers.

Figure 6-5: European dependency by technology sector 2022



Source: German Council on Foreign Relations via Statista (2022). Survey period January and February 2021, n=126. Respondents: Experts dealing with European technology and digital policy in government.

Figure 6-6: Desired aspects when purchasing cloud services - worldwide 2020

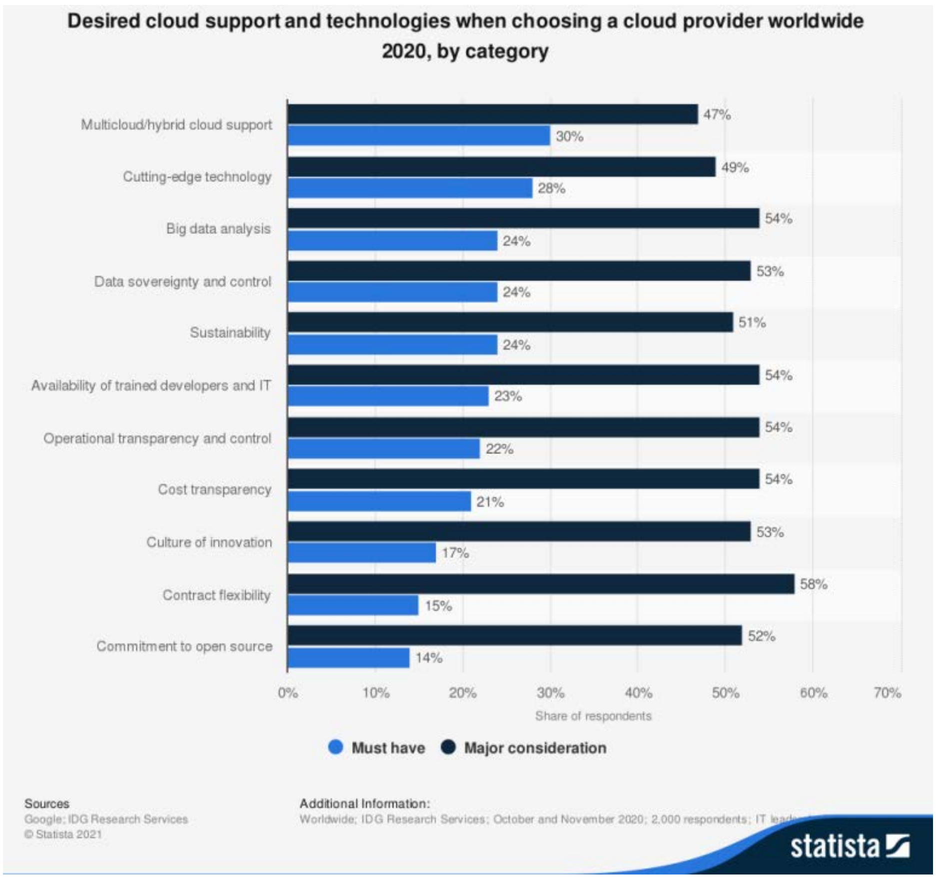
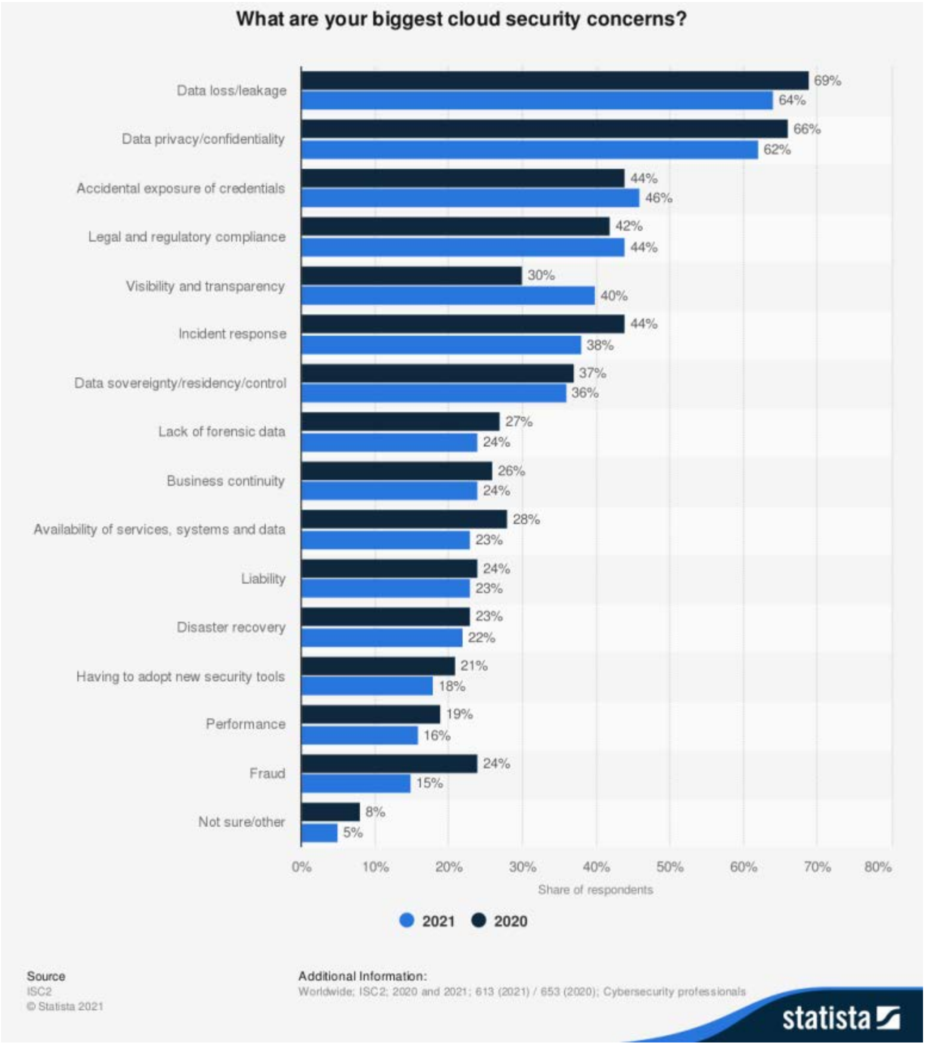


Figure 6-7: Biggest security concerns for cloud services - worldwide 2021-2022



Several conclusions can also be drawn under the aspect of competition:

- If governments impose local/national data requirements for cloud services, this would mean that the cloud provider would have to operate a data centre in each country where it offers its services. These "local" data centre requirements could become a barrier to entry for smaller cloud providers and would tend to limit economies of scale.
- In practice, end customers will look for the best services they can get for their money and will therefore most likely fall back on the already dominant providers and further consolidate their market position.

Is GAIA-X too late?

GAIA-X has been proposed as an alternative to US cloud providers for the European region. This is a project initiated in 2019 by France and Germany for the whole of Europe to advocate for and develop a common European data infrastructure. GAIA-X aims to develop a competitive, efficient and secure federation of (cloud) service providers for Europe to achieve greater independence from large cloud providers outside the EU.

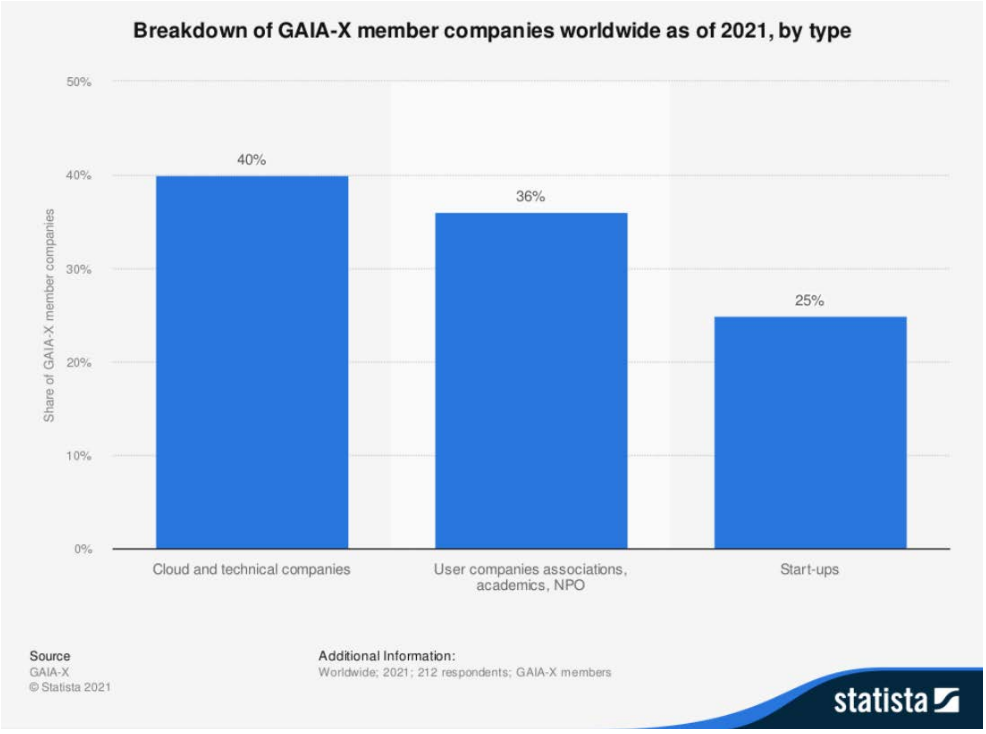
This "ecosystem" would also allow the sharing of data by European companies to develop new services. It also takes into account the laws of the countries where the companies hosting and processing the data are located. By encouraging European companies to use domestic cloud services, GAIA-X aims to reclaim data sovereignty so that data generated in Europe remains subject to European data protection law.

The BMWi (2021) states in its current study on digital sovereignty with regard to GAIA-X: "Der erfolgreichen Umsetzung einhergehend mit einer breiten Marktakzeptanz von GAIA-X kommt eine Schlüsselstellung zu, insbesondere da Unternehmen den Aspekt der Datenhoheit für ihr Unternehmen als sehr wichtig bewerten.“ [The successful implementation of GAIA-X in conjunction with broad market acceptance is of central importance, as companies consider the aspect of data sovereignty to be very important for their business.]. Allerdings sorgt die Mitgliedschaft von großen US-Unternehmen wie Amazon, Google und Microsoft bei GAIA-X auch für Besorgnis, dass die ursprünglichen Ziele im Hinblick auf mehr digitale Souveränität und weniger Abhängigkeit von großen außereuropäischen Technologiekonzernen nicht mehr erreicht werden könnten.[152]

According to Statista, 212 companies have joined this initiative as of March 2021, 92% of which are European companies. The following figure shows the categorisation of the joining organisations: 40% are cloud and technical providers. 36% are user companies, associations, academics or non-profit organisations, while 25% are start-ups.

152 Thyen (2021).

Figure 6-8: Composition of the GAIA-X Data Alliance 2021



It should be borne in mind that the large cloud providers started early in this business area and have continued to invest massively in their services and the associated global presence for years. End customers will opt for the services with the best price-performance ratio, which will most likely consolidate the dominant position of the US cloud providers in Europe for the time being.

In addition, there is a "lock-in" effect to consider: once business customers have chosen a particular cloud provider, the company incurs costs for the initial setup and learning how to use it. In addition, it is likely that these providers offer more than just cloud services, which can further increase the lock-in effect. This was also discussed in the Impact Assessment for the European Commission on the proposed Digital Markets Act.[153] Therefore, it is unlikely that companies that have already chosen a non-European cloud provider will easily consider switching to a solution from a European provider in the short term.

153 European Commission (2020a). Case study 3 on unjustified tying and bundling of office and cloud services by Microsoft leading to switching barriers.

6.7 Impact on European end consumers

Some of the aforementioned developments in the IP peering and transit markets may have negative consequences for end-users, such as a price premium through a CAP in the case of paid peering, but also positive ones such as the improved quality of CAP services through the use of CDNs. From a digital sovereignty perspective, however, the main aspects are about privacy and the security of end-users' data. The focus here is on transparency and control over where one's own user data is routed, processed and stored.

Transparency for end-users with regard to the forwarding of personal data and data security

In Section 6.5.1, the potential problems with user data routed through the US and therefore covered by US Cloud Law have already been discussed. This topic feeds into several ongoing discussions:

- Meta, Facebook's parent company, recently wrote in its 2021 annual report to the US Securities and Exchange Commission that it was essential to its business to allow users to transfer data back and forth between different countries. However, European data protection regulations prohibit the company from doing so and could therefore impact the availability of social networks in Europe. Meta hopes to reach an agreement with EU countries, but if this fails, possible discontinuation of services like Facebook or Instagram in Europe cannot be ruled out. Markus Reinisch, Meta's Vice President of Public Policy Europe, was quick to put this news into perspective; „Meta droht absolut nicht damit, Europa zu verlassen“ [*Meta is absolutely not threatening to leave Europe*], but „… die einfache Realität ist, dass Meta, wie viele andere Unternehmen, Orgaisationen und Dienstleistungen, auf Datenübertragungen zwischen der EU und den USA angewiesen ist, um unsere globalen Dienste zu betreiben.“ [...*the simple reality is that Meta, like many other companies, organisations and services, relies on data transfers between the EU and the US to run our global services.*][154]
- According to the CAPs we interviewed, their cache servers in the networks of European ISPs do not contain personalised user data. Although this information could not be further verified, it is conceivable that profile data of European end-users and/or metadata about content preferences are collected in European regions and transferred abroad.

154 Schwarzer (2022).

- Apple's recently announced Private Relay feature is about encrypting DNS requests from Safari browser sessions and a small subset of app traffic.[155] Although Private Relay is sometimes understood as an alternative to commercial VPNs, it is not a complete substitute, as user data can still be routed via the US (and fall under the US Cloud Act, which allows tapping by US intelligence).[156] Transparency to end users seems important in this regard. In the course of the implementation of Apple Private Relay, there have been complaints from European telecoms providers that advanced network features such as content filtering, zero-rating and traffic management have been compromised, thus limiting Europe's digital sovereignty.[157] However, Wired quotes an IT security expert on this who considers the restrictions on the underlying transport service of ISPs to be negligible.[158]

In this context, the approach of the Finnish NRA Traficom is interesting. Traficom explained in our interview that it is a principle for data protection reasons that user data remain in Finland. When this data leaves Finland through (re)routing, ISPs are supposed to inform their end customers. Traficom has included this in its broader guidelines. Both the ISP's obligation to inform the end customer and the guidelines increase transparency and end-users' awareness of their data.

In Section 6.5.1, we also discussed the concept of geographic routing versus encryption and concluded that it is more beneficial for the end user to encrypt their traffic than to restrict it geographically.

The European Commission published the results of the public consultation on the Data Act on the protection of personal data in 2021. According to Margrethe Vestager, Vice-President of the Commission, Europe's initiative ensures fairness by giving citizens and businesses better control over data sharing in line with European values. The Data Act aims to clarify for consumers and businesses in the EU who can use and access which data and for what purposes. In doing so, the Data Act ties in with the Data Governance Act, which is intended to strengthen trust and facilitate the sharing of data within the EU and between sectors.[159]

155 According to Apple's technical description (Apple 2021), there are two cascaded proxy servers. The first proxy server exchanges the user's IP address for a localised one from Apple and forwards the encrypted DNS query to the second proxy server outside the Apple network. The second proxy server now receives the decrypted DNS query with the IP address assigned by Apple. It should be noted here that only components are encrypted (Safari, DNS queries, partial app traffic) and no system-wide encryption of the traffic emerge from the description. Thus, two essential functionalities of a commercial VPN are not given, but in comparison to proxy servers, it goes beyond the functionality of these.

156 Hodge (2022).

157 See Fatih (2022) and Burgess (2022).

158 Wired (2022).

159 European Commission (2021a).

European Commission initiative to update cybersecurity rules

In December 2020, the European Commission proposed the revised Network and Information Security Directive (NIS2), which aims to extend existing cybersecurity rules.[160] This proposal may impact key internet infrastructures such as Domain Name Servers (DNS), Trust Services Providers and Certification Authorities in Europe. This has implications for routing of browser traffic, verification of digital identities and security certificates, among others.

The Internet Society responded with an Internet Impact Brief recommending that the European Commission exclude Root Name Servers as this runs counter to an open and neutral internet, and that the Commission conduct a comprehensive impact assessment to avoid unintended consequences.[161]

Recently, the European Commission launched a call for tender to study the initiative to establish a European infrastructure for DNS resolver services (called DNS4EU for short).[162] The European Commission considers this an important issue as citizens and organisations in the EU are increasingly reliant on public DNS resolvers operated by non-EU companies. For the most part, however, users will rely on their ISP's DNS and will not change it. In addition, however, there are several DNS servers operated by European associations.[163] Cloudflare explains DNS as the "phone book of the internet"; when users type domain names like "google.com" into web browsers, DNS is responsible for finding the correct IP address for those websites. Browsers then use these addresses to communicate with origin servers or CDN edge servers to access website information.[164]

Self-determination over digital identities

After transparency for end-users in terms of routing and security, it is desirable, in the interest of the digital sovereignty of the individual, that the end-user can decide when, how and for what purpose personal data is transmitted.

In this regard, Urbach (2022) proposes the concept of self-sovereign identities to meet the current challenges of digital identity management and at the same time take into account the requirements of digital sovereignty. Digital identities play an increasingly central role in the use of digital services and also in the analogue world. Urbach recommends that users, as central managers of their respective digital identities, should be able to maintain control over their identity across different services and thus gain autonomy in managing these services.

---

160 European Commission (2020b).
161 Meier-Hahn, U. (2017).
162 European Commission (2021b).
163 For example DNS server from digital courage, see https://digitalcourage.de/support/zensurfreier-dns-server
164 https://www.cloudflare.com/de-de/learning/dns/what-is-a-dns-server/

This concept is already being discussed, tested and implemented in various initiatives at regional, national and international level. Challenges addressed are the technical, professional and legal standardisation for the long-term interoperability of such systems, but also strengthening the competence of the user. Furthermore, the author points out that these systems should be based on common applications that are accessible to and used by all, as previous initiatives have shown that digital solutions only add value in the context of ecosystems with a strong user base.

Stable solutions for (business) end users

Last but not least, commercial users for whom internet access is crucial (or has become crucial during the pandemic) have started to interconnect directly at a regional IXP. Examples include companies in the education, insurance or financial sectors. From our interviews we could see that this is especially the case in the Netherlands, but is also the case in Germany. Stakeholders assume that this trend will continue, as during the pandemic, companies experienced that the quality of the connection to the IXP was better. This supports the conclusion drawn earlier that the availability of public peering at IXPs is relevant (see Section 6.5.2).

Bibliography

Abecassis, D. & Kende, M. (2020). "IP interconnection on the internet: a white paper". Analysys Mason. Retrieved from: https://www.analysysmason.com/consulting-redirect/reports/ip-interconnection-korea-white-paper/ .

Abecassis, D., Morgan, R. & Osman, S. (2018). "Infrastructure Investment by Online Service Providers". Retrieved from: https://www.analysysmason.com/consulting-redirect/reports/online-service-providers-internet-infrastructure-dec2018/ .

ACM (2021). "Marktstudie IP interconnectie 2021". Retrieved from: https://www.acm.nl/nl/publicaties/marktstudie-ip-interconnectie-2021 .

Ahmed, A., Shafiq, Z., Bedi, H. & Khakpour, A. (2017). Peering vs. Transit: Performance Comparison of Peering and Transit Interconnections. 2017 IEEE 25th International Conference on Network Protocols (ICNP), IEEE.

Akamai (2021a). "Facts and Figures". Access Date: 23.11.2021. Retrieved from: https://www.akamai.com/de/company/facts-figures.

Akamai (2021b). "Third Quarter 2021 Financial Results". Access Date: 28.11.2021. Retrieved from: https://www.ir.akamai.com/static-files/886ffbb3-1620-4030-8ef5-1f6d93f44619

Altomare, F. (2021). "Content Delivery Network Explained". GlobalDots. Retrieved from: https://www.globaldots.com/resources/blog/content-delivery-network-explained/ .

AMS-IX (2021). "Total Stats - AMS-IX Amsterdam". Retrieved from: https://stats.ams-ix.net/historical.html?start=201701;year=5.

Apple (2021). "iCloud Private Relay Overview". Retrieved from: https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF .

ARCEP (2021). "The state of the internet in France". Retrieved from: https://en.arcep.fr/uploads/tx_gspublication/report-state-internet-2021-edition-july2021.pdf .

Arnold, T., He, J., Jiang, W., Calder, M., Cunha, I., Giotsas, V. & Katz-Bassett, E. (2020). Cloud Provider Connectivity in the Flat Internet. Proceedings of the ACM Internet Measurement Conference: 230-246.

BEREC (2012a). "An assessment of IP interconnection in the context of Net Neutrality". Retrieved from: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/1130-an-assessment-of-ip-interconnection-in-the-context-of-net-neutrality .

BEREC (2012b). "BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines". Retrieved from: https://berec.europa.eu/eng/document_register/subject_matter/berec/others/1076-berecs-comments-on-the-etno-proposal-for-ituwcit-or-similar-initiatives-along-these-lines.

BEREC (2017). "BEREC Report on IP-Interconnection practices in the Context of Net Neutrality". Retrieved from: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/7299-berec-report-on-ip-interconnection-practices-in-the-context-of-net-neutrality.

BEREC (2020). "BEREC Guidelines on the Implementation of the Open Internet Regulation." Retrieved from: 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 .

BEREC (2021). "BEREC Summary Report on the status of internet capacity, regulatory and other measures in light of the Covid-19 crisis". Retrieved from: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/9993-berec-summary-report-on-the-status-of-internet-capacity-regulatory-and-other-measures-in-light-of-the-covid-19-crisis .

BMWi (2021). "Schwerpunktstudie Digitale Souveränität - Bestandsaufnahme und Handlungsfelder". Retrieved from: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.html

Böttger, T., Antichi, G., Fernandes, E. L., di Lallo, R., Bruyere, M., Uhlig, S., Tyson, G. & Castro, I. (2019). "Shaping the Internet: 10 Years of IXP Growth". arXiv:1810.10963 [cs].

Böttger, T., Ibrahim, G. & Vallis, B. (2020). How the Internet reacted to Covid-19. Proceedings of the ACM Internet Measurement Conference: 34-41.

Boudreau, B. (2021). Around the World in 20 Minutes: A Global Pricing Update. PTC 2021, TeleGeography.

Budnitsky, S. (2017). "Milton Mueller, Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace". International Journal of Communication 11(0): 5.

Bundesnetzagentur (2017). "Bundesnetzagentur sichert Netzneutralität - Teilaspekte von „StreamOn“ werden untersagt". Pressemitteilung. Retrieved from: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Presse/Pressemitteilungen/2017/15122017_StreamOn.pdf;jsessionid=C71B356569ADBF862690E9B1E9CF11C1?__blob=publicationFile&v=2

Bundesverwaltungsgericht Schweiz (2020). Urteil im Rechtsstreit Init7/Swisscom/ComCom im Fall A-5235/2018 bezüglich Interconnecton/Peering vom 22.04.2020.

Burgess, M. (2022). "Apple’s Private Relay Roils Telecoms Around the World". Wired. Retrieved from: https://www.wired.com/story/icloud-private-relay-blocking/ . Access Date: 17.02.2022.

Calvanese Strinati, E., Barbarossa, S., González-Jiménez, J. L., Kténas, D., Cassiau, N., Maret, L. & Dehos, C. (2019). "6G: The Next Frontier: From Holographic Messaging to Artificial Intelligence Using Subterahertz and Visible Light Communication". IEEE Vehicular Technology Magazine 14: 42-50.

Cisco (2019a). "Data volume of global content delivery network internet traffic from 2017 to 2022 (in exabytes per month)".

Cisco (2019b). "Global consumer IP traffic by region 2022". Statista. Access Date: 30.11.2021. Retrieved from: https://www.statista.com/statistics/267199/global-consumer-internet-traffic-by-region/ .

Cisco (2020). "Cisco Annual Internet Report (2018–2023)". Retrieved from: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html .

Clark, M. (2022). "The cost of ripping and replacing Chinese cellular equipment has ballooned by billions". The Verge. Retrieved from: https://www.theverge.com/2022/2/4/22918611/rip-and-replace-hauwei-zte-fcc-cell-network-securty . Access Date: 10.02.2022.

Coll, N. (2021a). "Unpacking European Wholesale Pricing". TeleGeography. Retrieved from: https://blog.telegeography.com/unpacking-european-wholesale-pricing-trends . Access Date: 26.11.2021.

Coll, N. (2021b). "A 2021 Check-In on Global IP Transit Price Trends". TeleGeography. Retrieved from: https://blog.telegeography.com/2021-global-ip-transit-price-trends . Access Date: 26.11.2021.

DE-CIX. (2021). "DE-CIX Frankfurt traffic statistics." DE-CIX. Access Date: 17.11.2021, Retrieved from: https://www.de-cix.net/en/locations/frankfurt/statistics .

Dey, P. K. & Yuksel, M. (2019). "Peering Among Content-Dominated Vertical ISPs". IEEE Networking Letters 1(3): 132-135.

DialogConsult (2021). "23. TK-Marktanalyse Deutschland 2021". Retrieved from: https://www.vatm.de/wp-content/uploads/2021/10/VATM_TK-Marktstudie_281021_f.pdf .

Doan, T. V., Bajpai, V. & Crawford, S. (2020). A Longitudinal View of Netflix: Content Delivery over IPv6 and Content Cache Deployments. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, IEEE.

Dönni, D., Sperb Machado, G., Tsiaras, C. & Stiller, B. (2015). "Schengen Routing: A Compliance Analysis". Universität Zürich, Institut für Informatik.

Draghi, M. (2019). Souveränität in einer globalisierten Welt. Europäische Zentralbank (EZB).

Economides, N. (2004). "The Economics of the Internet Backbone". NET Working Paper Series(04-23): 373-412.

Engebretson, J. (2019). "Behind the Level 3- Comcast Peering Settlement". TeleCompetitor. Access Date: 15.01.2022. Retrieved from: https://www.telecompetitor.com/behind-the-level-3-comcast-peering-settlement/ .

ETNO (2012a). "ITRs Proposal to Address New Internet Ecosystem". Retrieved from: https://etno.eu/datas/itu-matters/etno-ip-interconnection.pdf.

ETNO (2012b), "Position Paper: ETNO response to BEREC Consultation on "An Assessment of IP-IC in the context of Net Neutrality" - BoR (12) 33. July 2021. Retrieved from: https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/627-response-by-etno-to-berec-2012-public-co_0.pdf .

ETNO (2021). "Joint CEO Statement: Europe needs to translate its digital ambitions into concrete actions". Retrieved from: https://etno.eu/news/all-news/717-ceo-statement-2021.html .

Euro-IX (2020). "Internet Exchange Points 2020 Report". Retrieved from: https://www.euro-ix.net/media/filer_public/cf/7c/cf7c8cb1-40c9-4e37-9d79-02b61ccc081e/ixp_report_2020_.pdf .

European Commission (2018). Commission Decision of 30/05/2018 declaring a concentration to be compatible with the common market (Case No COMP/M.7000 - Liberty Global plc / Ziggo N.V. / Vodafone Group Plc) according to Council Regulation (EC) No 139/2004

European Commission (2019a). Commission Decision of 18/07/2019 declaring a concentration to be compatible with the common market (Case COMP/M.8864 - Vodafone Group Plc / Certain Liberty Global Assets) having regard to Council Regulation (EC) No 139/2004.

European Commission (2019b). Commitments tot he European Commissio in the Case M.8864.

European Commission (2020a). "Digital Markets Act: impact assessment support study: executive summary and synthesis report". Publication Office.

European Commission (2020b). "Revised Directive on Security of Network and Information Systems (NIS2)".

European Commission (2021a). "Data Act: Unternehmen und Bürger für eine faire Datenwirtschaft | Die digitale Zukunft Europas gestalten".

European Commission (2021b). "Connecting Europe Facility (CEF), Aufforderung zur Einreichung von Vorschlägen, CEF 2 Digital - Backbone networks for pan European cloud federation (CEF-DIG-2021-CLOUD), Version 1.0, 12. Januar 2022".

European Court of Justice (2021). Judgement of the Court (Eighth Chamber) from 2. September 2021. Telekom Deutschland GmbH vs Bundesrepublik Deutschland. Reference for a preliminary ruling – Electronic communications – Regulation (EU) 2015/2120 – Article 3 – Open internet access – Article 3(1) – End users' rights – Article 3(2) – Prohibition of agreements and commercial practices limiting the exercise of end users' rights – Article 3(3) – Obligation of equal and non-discriminatory treatment of traffic – Possibility of implementing reasonable traffic management measures – Additional 'zero tariff' option – Limitation on bandwidth. Case C-34/20, European Court of Justice.

Facebook (2021). "Advancing connectivity between the Asia-Pacific region and North America". Engineering at Meta. Retrieved from: https://engineering.fb.com/2021/03/28/connectivity/echo-bifrost/ . Access Date: 23.11.2021.

Fatih, S. (2022). "EU Mobile Operators Want Apple's iCloud Private Relay Service to Be Outlawed Over Concerns of 'Digital Sovereignty'". MacRumors. Retrieved from: https://www.macrumors.com/2022/01/10/eu-mobile-operators-icloud-private-relay/ . Access Date: 17.02.2022.

Feldmann, A., Gasser O., Lichtblau F., Pujol, E., Poese I., Dietzel C., Wagner D.Wichtlhuber, M., Tapiador, J., Vallina-Rodriguez, N., Hohlfeld, O. & Smaragdakis, G. (2021). "A year in lockdown". Communications of the ACM 64(7): 101-108.

Gallimore, D. (2021a). "IP Interconnection Portfolio". Liberty Global. Retrieved from: https://www.libertyglobal.com/operations/business-services/ip-interconnection-portfolio/ .

Gallimore, D. (2021b). "Global Peering Principles". Liberty Global. Retrieved from: https://www.libertyglobal.com/operations/business-services/global-peering-principles/ .

Gartner (2021). "Gartner Says Worldwide IaaS Public Cloud Services Market Grew 40.7% in 2020, Amazon, Microsoft and Alibaba Led the 2020 Race to the Cloud". Retrieved from: https://www.gartner.com/en/newsroom/press-releases/2021-06-28-gartner-says-worldwide-iaas-public-cloud-services-market-grew-40-7-percent-in-2020 . Access Date: 02.02.2022.

Goetz, D. (2019). "Dynamic Bargaining and Size Effects in the Broadband Industry". SSRN Electronic Journal.

Google (2021a). "New Apricot subsea cable brings more connectivity to Asia". Google Cloud Blog. Retrieved from: https://cloud.google.com/blog/products/infrastructure/new-apricot-subsea-cable-brings-more-connectivity-to-asia/ . Access Date: 26.11.2021.

Google (2021b). "Google Fiber". Retrieved from: https://fiber.google.com/ .

Heise online (2022). "Privatsphärenschutz: Warum sich Netzbetreiber gegen Apples Private Relay stellen". c't Magazin. Retrieved from: https://www.heise.de/news/Privatsphaerenschutz-Warum-sich-Netzbetreiber-gegen-Apples-Private-Relay-stellen-6335268.html . Access Date: 17.02.2022.

Hellberg, N. (2019). "Why Internet Routing Affects Digital Sovereignty". Retrieved from: https://www.trendmicro.com/vinfo/us/security/news/online-privacy/why-internet-routing-affects-digital-sovereignty . Access Date: 11.02.2022.

Herman, B. D. (2006). "Opening bottlenecks: On behalf of mandated network neutrality". Fed. Comm. LJ 59: 103.

Hetzner (2020). "Ab sofort direktes Peering mit der Deutschen Telekom". Retrieved from: https://www.hetzner.com/de/news/03-20-dtag/?country=de .

Hildén, J. (2021). "Mitigating the risk of US surveillance for public sector services in the cloud". Internet Policy Review 10(3).

Hjembo, J. (2019). Beyond the Hype. PTC 2019, TeleGeography.

Hodge, R. (2022). No, Apple's Private Relay is not a VPN, but you can still try it out with iOS 15. CNET.

Kagermann, H., Streibich, K.-H. & Suder, K. (2021). "Digitale Souveränität. Status quo und Handlungsfelder". Deutsche Akademie der Technikwissenschaften (acatech).

KPMG (2021). "The European Cloud market: key challenges for Europe and five scenarios with major impacts by 2027-2030".

Krämer, J., Wiewiorra, L. & Weinhardt, C. (2013). "Net neutrality: A progress report". Telecommunications Policy 37(9): 794-813.

Kroon, P., Baischew, D., Lucidi, S., Märkel, C. & Sörries, B. (2020). "Digital Sovereignty in Europe - a first benchmark". WIK Consult.

Kuch, A. (2015). Anbindung an Telekom: Schnelles Netz kostet extra (Update: Telekom). Teltarif. Retrieved from: https://www.teltarif.de/double-paid-traffic-telekom-hetzner/news/61976.html .

Kwang, H. R., Park, J. E. & Kim, D. I. (2021). "Korean court ruling over a network usage fee dispute between Netflix and SK Broadband". Chambers and Partners. Retrieved from: https://chambers.com/articles/korean-court-ruling-over-a-network-usage-fee-dispute-between-netflix-and-sk-broadband .

Labovitz, C. (2019). Internet Traffic 2009-2019. NANOG 2019.

Lee, J. (2021). "S.Korea broadband firm sues Netflix after traffic surge from 'Squid Game'". Reuters. Retrieved from: https://www.reuters.com/business/media-telecom/skorea-broadband-firm-sues-netflix-after-traffic-surge-squid-game-2021-10-01/ .

Limelight (2021). "Limelight Networks: Network Map". Retrieved from: https://de.limelight.com/network-map/ .

Lyons, D. A. (2018). "An Antitrust-Informed Approach to Regulating Internet Interconnection". Journal of Science & Technology Law 24(2): 229-276.

Marcus, J. S. (2014). "The Economic Impact of Internet Traffic Growth on Network Operators". SSRN Electronic Journal.

Meier-Hahn, U. (2017). "The secrets of de-peering – Digital Society Blog". HIIG. Retrieved from: https://www.hiig.de/en/the-secrets-of-de-peering/ .

Miller, J. (2021). "2021 Global Pricing Trends in 20 Minutes". Telegeography. Retrieved from: https://blog.telegeography.com/2021-global-pricing-trends-in-20-minutes .

Mitchell, C. (2022). "Die Kosten für das Abreißen und Ersetzen chinesischer Mobilfunkgeräte haben sich um Milliarden erhöht". The Verge, 4. Februar 2022. Retrieved from: https://www.theverge.com/2022/2/4/22918611/rip-and-replace-hauwei-zte-fcc-cell-network-securty

Mozilla Foundation (2019). "The new investors in underwater sea cables". The Internet Health Report 2019. Retrieved from: https://internethealthreport.org/2019/the-new-investors-in-underwater-sea-cables/ .

Netflix (2021a). "A cooperative approach to content delivery - A Netflix briefing paper 2021". Retrieved from: https://openconnect.netflix.com/Open-Connect-Briefing-Paper.pdf .

Netflix (2021b). "Response to Ofcom Consultation from 01.11.2021". Nicht veröffentlicht.

Nikkhah, A. & Jordan, S. (2021). "The Effect of Paid Peering Fees on Broadband Prices and Consumer Surplus". SSRN Electronic Journal.

OECD (2020). "Keeping the Internet up and running in times of crisis". Retrieved from: https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/ .

Ofcom (2016). "Connected Nations 2016". Retrieved from: https://www.ofcom.org.uk/research-and-data/multi-sector-research/infrastructure-research/connected-nations-2016 .

Ofcom (2017). "Connected Nations 2017 - Detailed analysis". Ofcom. Retrieved from: https://www.ofcom.org.uk/research-and-data/multi-sector-research/infrastructure-research/connected-nations-2017/main-report .

OnVista (2021a). "Meta Platforms (ehem. Facebook) Aktie". onvista.de. Retrieved from: https://www.onvista.de/aktien/Meta-Platforms-ehem-Facebook-Aktie-US30303M1027 .

OnVista (2021b). "Netflix Aktie". onvista.de. Retrieved from: https://www.onvista.de/aktien/Netflix-Aktie-US64110L1061 .

Open Net Korea (2020). "Open letter to South Korea's ICT Minister: ensure Net Neutrality". Access Now. Retrieved from: https://www.accessnow.org/open-letter-south-korea-net-neutrality/ .

Park, K. S. & Nelson, M. R. (2021). "Afterword: Korea’s Challenge to the Standard Internet Interconnection Model”. In: The Korean Way With Data: How the World’s Most Wired Country Is Forging a Third Way. Carnegie Endowment for International Peace. Retrieved from: https://carnegieendowment.org/2021/08/17/afterword-korea-s-challenge-to-standard-internet-interconnection-model-pub-85166 . Access Date: 26.11.2021.

Pauker, M. (2021). "Netflix: 500 Millionen für lokalen Content". W&V. Retrieved from: https://www.wuv.de/medien/netflix_500_millionen_fuer_lokalen_content .

PeeringDB (2021a). "Eintrag der Deutschen Telekom (AS3320)". Retrieved from: https://www.peeringdb.com/net/196 .

PeeringDB (2021b). "Database Backup from 01.11.2021". Retrieved from: https://www.peeringdb.com/ .

Pohle, J. (2020). "Digitale Souveränität - Ein neues digitalpolitisches Schlüsselkonzept in Deutschland und Europa". Konrad Adenauer Stiftung.

Pohlmann, N., Sparenberg, M., Siromaschenko, I., & Kilden, K. (2015). "Sichere Kommunikation und digitale Souveränität in Europa". Institut für Internet-Sicherheit - if(is) Westfälische Hochschule, Gelsenkirchen University of Applied Sciences.

Poitras, L, Rosenbach, M. und Stark, H. (2013). „NSA überwacht 500 Millionen Verbindungen in Deutschland“. Der Spiegel, 30. Juni 2013. Retrieved from: https://www.spiegel.de/netzwelt/netzpolitik/nsa-ueberwacht-500-millionen-verbindungen-in-deutschland-a-908517.html.

Qualcomm (2018). "VR and AR pushing connectivity limits".

Reilly, K. (2019). "Checking In: Yup. Price Erosion is Still Very Real." TeleGeography. Access Date: 28.11.2021. Retrieved from: https://blog.telegeography.com/yup.-price-erosion-is-still-a-thing .

Rimol, M. (2021). "Gartner Says Worldwide IaaS Public Cloud Services Market Grew 40.7% in 2020". Gartner. Retrieved from: https://www.gartner.com/en/newsroom/press-releases/2021-06-28-gartner-says-worldwide-iaas-public-cloud-services-market-grew-40-7-percent-in-2020 .

RND (2022). "Bald kein Facebook und Instagram mehr? Meta-Konzern droht Europa". Retrieved from: https://www.rnd.de/digital/bald-kein-facebook-und-instagram-mehr-meta-droht-europa-SYDNGQZ55FDA5GUWZMLEYR2SOA.html . Access Date: 09.02.2022.

Sandvine (2014). "Global Internet Phenomena Report 2H - 2014". Retrieved from: https://www.sandvine.com/hubfs/downloads/archive/2014-2h-global-internet-phenomena-report.pdf .

Sandvine (2020). "COVID Internet Phenomena Report Spotlight". Retrieved from: https://www.sandvine.com/covid-internet-spotlight-report .

Schlinker, B., Kim, H., Cui, T., Katz-Bassett, E., Madhyastha, H. V., Cunha, I., Quinn, J., Hasan, S., Lapukhov, P. & Zeng, H. (2017). Engineering Egress with Edge Fabric. Proceedings of the Conference of the ACM Special Interest Group on Data Communication: 418-431.

Schwarzer, M. (2022). "Facebook-Rückzug aus Europa? Das wäre problematischer, als man denkt". RND. Retrieved from: https://www.rnd.de/medien/meta-facebook-rueckzug-aus-europa-wo-liegt-das-problem-LYDICI6VQJDSNK4DVSAFHYKJNY.html . Access Date: 15.02.2022.

Serentschy, G. (2021). "Innovation and Regulation in the Digital Communications Field." Serentschy.com. Retrieved from: https://www.serentschy.com/the-regulatory-journey-from-a-european-perspective/ . Access Date: 26.11.2021.

Snijders, J., Abdel-Hafez, S., Strong, M., Alom, C. & Stucchi, M. (2021). "IXP Megabit/Sec Cost & Comparison". Peering.exposed. Retrieved from: https://peering.exposed .

Song, S. (2019). "Internet Drift: How the Internet Is Likely to Splinter and Fracture". Digital Freedom Fund, Retrieved from: https://digitalfreedomfund.org/internet-drift-how-the-internet-is-likely-to-splinter-and-fracture/ .

Sowell, J. H. (2020). "Evaluating competition in the Internet's infrastructure: a view of GAFAM from the Internet exchanges". Journal of Cyber Policy 5(1): 107-139.

Thyen, A.E. (2021). „Haben wir noch eine Chance auf digitale Selbstbestimmung?". it-daily.net. Retrieved from: https://www.it-daily.net/it-management/digitalisierung/31522-haben-wir-noch-eine-chance-auf-digitale-selbstbestimmung. Access Date: 25.02.2022.

Van der Berg, R. (2021). "T-Mobile NL routed all internet traffic through Germany and broke the Internet for small firms". Medium. Retrieved from: https://rudolfvanderberg.medium.com/t-mobile-nl-routed-all-internet-traffic-through-germany-and-broke-the-internet-for-small-firms-a176855d2b0 .

Voge, C., Kolkman, O. & Robachevsky, A. (2021). "Internet Impact Brief: Revised Directive on Security of Network and Information (NIS2) – Presidency Compromise Proposal September 2021". Internet Society.

Wang, X. & Ma R. T. B. (2020). "On the Tussle Between Over-the-Top and Internet Service Providers: Analysis of the Netflix- Comcast Type of Deals". IEEE/ACM Transactions on Networking 28(6): 2823-2835.

WEKO (2014). "Gutachten im Fall 533.1-0021 zu Interconnect/Peering".

Weller, D. & Woodcock, B. (2013). "Internet Traffic Exchange: Market Developments and Policy Challenges". Retrieved from: https://www.oecd-ilibrary.org/science-and-technology/internet-traffic-exchange_5k918gpt130q-en .

Woodcock, B. & Frigino, M. (2016). "2016 Survey of Internet Carrier Interconnection Agreements". Retrieved from: https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6574-2016-survey-of-internet-carrier-intercon_0.pdf .

Appendix 1: Evaluation of the online survey of IRG members

1. Conducting the survey

In order to obtain a broad European market overview for the identification of regulatory interventions in the IP transit and peering markets as well as to obtain assessments on Digital Sovereignty, we conducted an online survey to all members of the Independent Regulators Group in the period 27 October to 15 November 2021. Of the 37 members of the IRG, 16 returned an evaluable questionnaire. The response rate was therefore 43%. The questions related to

- Market development,
- Transport development,
- IP Interconnection Disputes,
- Digital sovereignty.

Not all respondents answered the questionnaire completely. In this respect, the survey does not provide a representative picture for Europe, taking into account the response rate. Nevertheless, we present here an evaluation of the responses, as a number of remarkable findings have emerged.

2. Market development

The vast majority of respondents (91%) report an increase in IP traffic in their country. 73% report a strong increase. CTU (CZ[165]) even reports a 600% increase in mobile traffic in four years. Many report a strong pandemic-related increase in traffic, which then remained at the higher level.

Video streaming is cited by most as the predominant driver of traffic growth. It is followed by the pandemic and cloud services, furthermore gaming, digitalisation and customer growth.

Few NRAs comment on transit prices, as this market is deregulated and therefore not monitored. Others have no corresponding market information. Concrete statements on price trends are usually made by NRAs that were involved in an IP interconnection dispute or conduct detailed market surveys (such as FR). Otherwise, price trends are reported to continue to fall. In NL, paid peering is said to have played a relatively large role in the last five years. Here, large CAPs have agreed better conditions than smaller ones.

165 In the following, the countries are abbreviated with their ISO 3166 Alpha 2 abbreviations, which also correspond to the TLDs.

No concrete information on CDN prices was available from the NRAs. However, CH and FR report falling prices here as well.

Most NRAs do not have any information or make any statements on the development of costs. Four NRAs argue that costs are (steadily) decreasing due to technical progress in components and as a result of economies of scale.

Only a few NRAs make statements on the relative importance of IP transit and peering. Several NRAs emphasise the importance of transit for connectivity and the importance of peering for quality. While FR reports a relative decline of transit, CH and NL assume that both forms of interconnection have developed in parallel. In NL, transit and peering have developed more at the expense of IXP traffic. (This also corresponds to the development in DE).

There are only a few statements on pricing in peering. NL, F and CH report an increasing amount of paid peering. In Switzerland, however, the share of settlement-free peering is (still) higher than that of paid peering.

Only a few NRAs report on the symmetry of traffic. In CH and F, a pandemic-related (slight) decrease in traffic asymmetry is reported. In NL, the trend of increasing asymmetry continues.

Just few NRAs comment on the incumbent's peering behaviour and peering policy. The reference to a selective/restrictive peering policy predominates. In PL the incumbent is present at the IXP. According to Swisscom's peering policy, private peering (among other conditions) is only offered with a traffic volume of 1 Gbps. A few years ago, the peering threshold was still 300 Mbps. Below this, public peering is offered with a minimum traffic volume of 50 Mbps. Swisscom requires a ratio of 1:2 for settlement-free peering. Furthermore, Swisscom only offers peering to ISPs whose backbone has a minimum size of 50% of Swisscom's capacity. In CZ, the incumbent is represented at several IXPs and states an open peering policy itself. We attribute this to structural separation and the wholesale-only approach. In the Netherlands, the incumbent KPN operates its own IXP NL-IX. This is accompanied by a withdrawal from the largest Dutch IXP AMS-IX. ARCEP reports that the ISPs in FR each operate different peering policies. Only two NRAs (IE, RS) expect the COVID pandemic to have a significant impact on the IP interconnection market. NO, FR, RO, SK assume that there is no significant impact.

3. Traffic via IXP

As many NRAs do not track or monitor IP interconnection markets, they do not make statements on the volumes of traffic exchanged via IXP. CZ, NL, NO, IT, FR, SK report increasing IXP traffic, with a decreasing relative share in FR. In NL, peek traffic p.a. is increasing by about 1 Tbps in recent years. Not all NRAs make statements on the incumbent's presence at IXPs. All respondents confirm that "their" incumbent is represented at the IXP. In NL, large ISPs also operate their own IXPs. These are measures to enforce paid peering. There is no information on the capacity with which incumbents are represented at IXPs.

4. IP Interconnection Disputes

Only CH, RS and IT report formal regulatory proceedings in IP interconnection matters in the last 5 years. The procedure in CH relates to the Init7/Swisscom procedure described in Section 5.2.1. The procedure in RS concerned an IP interconnection dispute between the incumbent and Altnets. The dispute was resolved by a regulatory requirement for national IP interconnection at the transit level.

No NRA reports its own involvement in dispute settlement in connection with IP transit and peering. Only for CH is there a report of intervention by the competition authority in the transit/peering market.

Only the NRAs from NL and FR report open disputes from market participants on IP transit and peering. In NO, NKom mentions another complaint from market participants about IP transit/peering. The dispute in NL was about insufficient capacity at the POI and traffic throttling. The complaint in NO was that an ISP did not want to host CAP/CDNs.

With regard to complaints from end customers about service quality problems, OFCOM points to the dispute between Netflix and Swisscom in 2016. Here peering disputes had led to quality restrictions, which then led the companies to an agreement. NO reports on a quality index of Netflix from 2012, in which Telenor scored the worst. This stems from disputes between Telenor and Netflix over the on-net placement of Netflix CDN servers on Telenor's network. Telenor refused to do so, citing its own network sovereignty. NL and FR also report customer complaints. In FR, these concern the performance of certain CAP services with the ISP Free in 2018. These problems were due to bottlenecks at a transit provider.

With regard to the incumbent's abuse of market power in peering and transit, OFCOM refers to the Init7/Swisscom case.

Appendix 2: Online questionnaire

Competitive issues of the transit and peering markets - implications for the digital sovereignty of Europe

The Federal Network Agency of Germany (BNetzA) recently commissioned a study on "Competitive issues of the transit and peering markets - implications for the digital sovereignty of Europe" to WIK-Consult. The study shall identify and assess major market trends in the European peering and transit markets over the last five years and the implications for the digital sovereignty in Europe.

The last comprehensive study on the IP interconnection market has been conducted by BEREC in 2017. This study is supposed to take BEREC's former findings and conclusions as a starting point.

This questionnaire is sent to all IRG members and will be a major and valuable input to the study. Given the existing intransparencies of the transit and peering market we expect that NRAs can rely on the best market insights and very much hope that you share this knowledge with us, the BNetzA and your IRG colleagues.

In case, there are confidential aspects of your responses, these can be marked in the text fields and will only be shared with the BNetzA but anonymised in the published report. Furthermore, the BNetzA intends to make the English version available to all IRG members in early 2022.

The complete questionnaire takes around 20 minutes to fill in.

Given the tough timeline of the study we kindly ask you to respond to this questionnaire not later than 15 November 2021. If you cannot answer all questions, we would be pleased to receive answers to those questions you are able to answer.

Thank you for your time!

In case you have questions in relation to this questionnaire feel free to contact Mr Lukas Wiewiorra (l.wiewiorra@wik.org or +49 2224 9225 025) or Mr Peter Kroon (p.kroon@wik.org or +49 (0)2224 922 558).

About Your Organisation
Do you work for the National Regulatory Authority? ☐ Yes ☐ No
What is the name of your organisation?
In which country are you active? If other, please specify.
Please provide your contact information. ☐ Name: ☐ Position ☐ Email ☐ Phone

Market Development
Which trends did you observe over the last five years regarding traffic volumes / growth rate of IP traffic in your country? What are the main drivers of these developments?
Which trends did you observe over the last five years regarding IP transit prices in your country?
Which trends did you observe over the last five years regarding CDN prices in your country?
Which trends did you observe over the last five years regarding the costs for the provision of IP-interconnection and CDN services (e.g. due to technological progress)?
What are your observations over the last five years on the relative importance of IP transit vs. IP peering in your country?

Which trends did you observe over the last five years regarding settlement-free and paid IP peering in your country?
Which trends did you observe over the last five years regarding traffic symmetry / asymmetry in your country?
What is the IP peering policy of your incumbent telecom operator? Has it changed over the last five years? ☐ Yes ☐ No ☐ I don't know / No answer If it has changed, please specify.
Has the COVID-19 pandemic had any decisive impact on the interconnection market in your country? ☐ Yes ☐ No ☐ I don't know / No answer If yes, please specify.

IXP Traffic Developments
What are your observations over the last five years regarding the traffic volumes exchanged over public IXPs in general and at peak traffic times?
Is your incumbent telecom operator interconnected at public IXPs? ☐ Yes ☐ No ☐ I don't know / No answer If yes, what is the capacity of these interconnections in relation to interconnections of the incumbent to other operators?

IP Interconnection Disputes
Did you have formal regulatory procedures regarding IP interconnection in the last five years? ☐ Yes ☐ No ☐ I don't know / No answer Please name the parties involved in the formal regulatory procedures regarding IP interconnection in the last five years. Please describe the outcome of the case/cases. Please provide reference to the case/cases.
Has your NRA been involved in any dispute settlement regarding IP transit/peering in the last five years? ☐ Yes ☐ No ☐ I don't know / No answer Please name the parties involved in any dispute settlement regarding IP transit/peering in the last five years. Please describe the subject and outcome of the case/cases. Please provide reference to the case/cases.
Has the Competition Authority in your country been involved in a legal case regarding IP transit/peering in the last five years? ☐ Yes ☐ No ☐ I don't know / No answer Please name parties involved in a legal case regarding IP transit/peering in the last five years. Please describe the subject and outcome of the case/cases. Please provide reference to the case/cases.

Are you aware of any open disputes between CDNs, CAPs, end-user ISPs, Backbone ISPs regarding IP transit/peering in the last five years?

- ☐ Yes
- ☐ No
- ☐ I don't know / No answer

Please name parties involved in the open disputes regarding IP transit/peering in the last five years (e.g. CDNs, CAPs, end-user ISPs, Backbone ISPs).

Please describe the subject and outcome of the case/cases.

Please provide reference to the case/cases.

Did you get (formal or informal) complaints from CAPs or ISPs regarding IP transit / peering in the last five years?

- ☐ Yes
- ☐ No
- ☐ I don't know / No answer

Please specify the issues at the core of the complaints from CAPs regarding IP transit / peering.

- ☐ Insufficient capacity at POIs
- ☐ Restrictive peering policy
- ☐ Traffic throttling
- ☐ Other
- ☐ I don't know / No answer

☐ If other, please specify.

Please specify the issues at the core of the complaints from ISPs regarding IP transit / peering.

- ☐ Insufficient capacity at POIs
- ☐ Restrictive peering policy
- ☐ Traffic throttling
- ☐ Other
- ☐ I don't know / No answer

☐ If other, please specify.

Did you get complaints from end-users regarding quality problems caused by IP transit/peering constraints in the last five years?

- ☐ Yes
- ☐ No
- ☐ I don't know / No answer

☐ If yes, please specify.

Are there any indications of abusive market behaviour of your incumbent telecom operator regarding IP peering/transit you are aware of?

- ☐ Yes
- ☐ No
- ☐ I don't know / No answer

☐ If yes, please specify.

Digital Sovereignty

In your view, what are the relevant dimensions of digital sovereignty?

- ☐ Cybersecurity
- ☐ Data protection
- ☐ Control over key technologies like AI, content, data centres, cloud computing etc.
- ☐ Strategic dimensions like the protection of European values, stakeholders, revenues, etc.
- ☐ I don't know / No answer

☐ If other, please specify.

If you selected the option "Control over key technologies like AI, content, data centres, cloud computing, etc.", please specify the key technologies in more detail.

- ☐ AI
- ☐ Content
- ☐ Data centres
- ☐ Cloud computing
- ☐ Other
- ☐ I don't know / No answer

☐ If other, please specify.

If you selected the option "Strategic dimensions like the protection of European values, stakeholders, revenues, etc.", please specify the strategic dimensions in more detail.

- ☐ Protection of European values
- ☐ Protection of European business value added
- ☐ Protection of European champions
- ☐ Protection of European tax revenues
- ☐ Other
- ☐ I don't know / No answer
- ☐

☐ If other, please specify.

Do you see issues in transit and peering markets in the context of digital sovereignty? Yes

- ☐ No
- ☐ I don't know / No answer

Please provide your reasoning.

Do you consider that any measures in respect of IP peering and transit are required to protect the digital sovereignty of Europe?

- ☐ Yes
- ☐ No
- ☐ I don't know / No answer

Have you considered the control of transit fees?

- ☐ Yes
- ☐ No
- ☐ I don't know / No answer

If yes, please explain why.

Have you considered the control of peering fees?

- ☐ Yes
- ☐ No
- ☐ I don't know / No answer

If yes, please explain why.

Have you considered European level intervention?

- ☐ Yes
- ☐ No
- ☐ I don't know / No answer

If yes, please explain why.

Have you considered other measures? If yes, please name the measures and explain why.

Which actions on the European level should be considered?

Schengen routing

- ☐ Market investigations
- ☐ Recommendations/Directives regarding IP traffic flows
- ☐ Dispute resolution process with multi-national companies
- ☐ Other
- ☐ I don't know / No answer

☐ If other, please specify.

Are there any governmental or parliamentary initiatives in respect to IP peering and transit in your country to protect digital sovereignty?

- ☐ Yes
- ☐ No
- ☐ I don't know / No answer

☐ If yes, please name the governmental or parliamentary initiatives and provide reference to relevant documents.

Appendix 3: Glossary

Autonomous systems:	Autonomous systems are understood to be a set of routers that route packets internally and externally according to a common policy and are technically managed from one location. Through technical progress and the flattening of network structures, the administration and the specified paths can now be managed more flexibly within an autonomous system. Externally, however, a coherent representation of the achievable paths and responsibility is recognisable.
Backbone ISP:	A backbone ISP is a network operator that maintains its network primarily for the purpose of business subleasing of capacity and offers connectivity between its own geographically highly differentiated locations as a product.
Bill-and-Keep Principle:	The bill-and-keep principle refers to a commercial relationship in the interconnection of networks in which both parties do not charge each other for the traffic volume exchanged between them.
Border Gateway Protocol (BGP):	BGP is a routing protocol that is used to connect autonomous systems. The autonomous systems connected via BGP mutually exchange the routes to the reachable addresses and renew them if necessary.
Cloud:	The term cloud or services realised in the cloud refers to the device-independent and thus location-independent provision of resources, in which the computing load is distributed across several servers. In terms of design, a distinction is usually made between the provision of infrastructures, platforms, software or functions. Cloud services can be realised purely privately (within a company), publicly or mixed.
Compound Annual Growth Rate (CAGR):	CAGR is the average annual growth rate, i.e. the linear slope between two measurement points.
Content and Applications Provider (CAP):	CAPs are service providers whose products consist of content (e.g. information, audiovisual media) and/or applications (e.g. programmes, games, mobile apps) that are provided digitally.
Content Delivery Network (CDN):	A CDN is a geographically differentiated network of connected servers that distribute the load by locally mirroring and storing frequently accessed content. This saves backbone capacities and improves the quality of the connection by shortening the paths. In addition to purely commercial CDN providers such as Akamai, there are increasingly CAPs that also maintain their own CDN structures in the course of the "make-or-buy" consideration (see Inhouse CDN).
Eyeball ISP:	An eyeball ISP is an ISP whose customers are end users (eyeballs) who consume content and whose connectivity is established via the ISP. This includes classic internet access providers with a focus on end customers.
Hosting Provider:	A hosting provider provides technical infrastructure to private and corporate customers. The scope ranges from ready-made software solutions for the provision of a website to virtual machines and complete servers. In all cases, the service of a hosting provider includes purchasing, connectivity and maintenance of the servers.

In-house CDN:	A CDN (see CDN) that is built, used and maintained internally by a CAP.
Internet Exchange Point (IXP):	IXP is an Internet node to which many autonomous networks are connected that can exchange data packets with each other. Although IXPs now also offer private peering services (see Private Peering), the original business field assumed in this framework is public peering between parties connected to the IXP. The connected parties pay a fixed price for a connection speed (e.g. 1 GigE, 10 GigE) but not variable prices for its utilisation. Annual membership fees can also be charged.
Label Edge Router (LER):	The function of LER is to identify packets based on their routing with a transport label within the network concerned.
Label Switch Router (LSR):	LSRs use the transport labels of the LER to transport the packet through the network according to the desired path.
On-Net CDN:	On-net CDNs are those parts of the CDN infrastructure that are not located at central transfer points (IXPs or data centres) but within the networks of ISPs. This can further shorten the paths for content delivery and relieve the interconnection capacities of the ISP and the CAP.
Open Connect Appliances (OCA):	OCA is Netflix's CDN infrastructure, which is provided to ISPs for installation within their own network (see On-Net CDN). The ISP is responsible for the location and the power consumption, Netflix takes over the costs of the hardware and the maintenance of the software.
Peering:	Peering is the direct interconnection of two autonomous systems for data exchange. Traditionally, peering has taken the form of a "settlement-free" or "bill-and-keep" agreement (especially between Tier 1 operators), in which no payments are foreseen between the parties. With increasing flexibility and flattening of the hierarchies, "paid" peering emerged alongside this, in which, for example, special requirements for quality and/or traffic volumes can be reflected in payments. Peering can take place at IXPs or co-locations/data centres (see Public and Private Peering).
PeeringDB:	PeeringDB is a publicly accessible database that gives interested parties the opportunity to specify public and private presences of autonomous systems. In addition to voluntary cooperation, PeeringDB also allows companies to enter their autonomous systems and presence points, as well as contact details and peering specifications.
Private Peering:	Private peering is a subset of peering that is not handled via a public IXP, but is represented in co-locations/data centres via cross-connects. In contrast to public peering, the connection speeds are usually not publicly communicated.
Public Peering:	Public peering is the common case of peering at public IXPs and refers to a publicly communicated connection to a node whose bandwidth can usually be used by all participants of the IXP under low requirements.

Tier 1 operators:	Tier 1 operators are a group of large network operators who, in turn, did not need transit to reach all Internet destinations. Tier 1 operators exchange traffic with each other via bill-and-keep peering and sell transit to Tier 2 operators. Lower tier 2 operators buy transit from tier 1 operators, peer predominantly with other tier 2 operators and in turn sell transit to tier 3 operators. Due to the flattened topology of the internet, these delineated classical hierarchies and business relationships are now only of limited validity.
Transit:	Transit refers to volume-based and paid connectivity to the internet via a transit provider (usually tier 1 provider). Transit thus differs from peering by volume-based billing and the accessibility of all routes on the internet through the interconnection.
Video on Demand (VoD):	VoD refers to the time-independent availability of a video, usually in connection with digital streaming offers. In this case, parts of the video are sent as a packet via an internet connection on demand for direct display.
Virtual Private Network (VPN):	A VPN is the direct, encrypted connection of a computer to a network, whereby all traffic is routed through the internet to the connected network. This makes it possible, for example, to establish an encrypted direct connection to the employer's network from the home office and to retrieve files in encrypted form. Calling up data outside the VPN is also routed from the computer via the company's private network to the internet and vice versa.