BEREC
Body of European Regulators
for Electronic Communications

BoR (24) 51

Draft BEREC Report on the entry of large content and application providers into the markets for electronic communications networks and services

7 March 2024

Contents

Executive Summary

Large content and application providers (CAPs) have traditionally provided services on the client and server sides of the internet ecosystem. However, in the last decades, large CAPs have become prominent actors in the internet ecosystem and have been investing increasingly in own infrastructures and providing services closely related to electronic communication networks (ECN) and electronic communication services (ECS), or directly qualifying as such. Some typical examples include content delivery networks (CDNs), the deployment of extensive international networks (e.g. submarine cables and satellite constellations), virtualised network services, cloud computing with increasing ubiquity, as well as trends towards the provision of internet access services.

This report gives an overview of the impact of large CAPs on the markets for ECN and ECS in Europe, by presenting their strategies, business models, and relations with traditional ECN/ECS providers in terms of competition, cooperation and interdependence. BEREC has already highlighted[1] how the accumulation of a significant variety of the internet ecosystem elements in the hand of a few Big Tech companies can have important consequences, such as leading to market concentration (as it is the case e.g. for cloud services, instant messaging, and operating systems), or affecting internet traffic and the decentralised approach on which the internet was created.

In order to better analyse the implications of the CAPs' presence and strategies in ECS/ECN markets, three case studies[2] focusing on CDNs, submarine cables and internet relay services[3], are carried out. Moreover, the report also highlights some potential restrictions that may be imposed by operating systems providers on ECN/ECS operators.

The commercial CDN services market in Europe currently appears to be concentrated around few players, as significant investments are required to have the necessary geographical coverage and capillarity to enter the market. Such concentration is expected to grow significantly in the coming years. Previously, large CAPs relied on commercial CDNs providers for their services, but in recent years they have been increasingly rolling out their own CDN infrastructure networks. They mostly use it for self-provision but also partly provide CDN services to third-parties, thus directly competing with commercial CDN providers. Moreover, on the one hand, the roll-out of CDNs by large CAPs – often on the internet service provider (ISP)'s network (i.e. on-net CDN) – exerts competitive pressure on the business model of transit providers; while on the other hand, on-net CDNs allow to reduce capacity costs for ISPs by locating content closer to end-users.

[1] BoR (22) 167, BEREC Report on the Internet Ecosystem, see: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-internet-ecosystem.

[2] This selection is not meant to exhaustively represent CAPs' presence and strategies in ECS/ECN markets.

[3] Services providing enhanced privacy features like tracking prevention (e.g. regarding IP-Addresses and DNS) or prevention of precise location determination. Such services include e.g. Apple iCloud Private Relay, Google One VPN or Microsoft Edge Secure Network.

Submarine fibre optic cables play a key role in maintaining a robust and high-capacity global network infrastructure: in 2023, they carried 99% of all international IP traffic, including the services provided by CAPs to consumers. The submarine cable ecosystem and the relations among stakeholders have significantly evolved in the last few years: large CAPs have transformed from mere direct or indirect customers of wholesale capacity, to the owners and investors in transport network infrastructure. The have become the driving force behind a significant portion of newly deployed high-capacity systems: they are currently responsible for more than 60% of the international traffic transits through submarine cables[4], and are able to lease capacity on some of their cables to the ECN/ECS providers. In this context, while large CAPs deploy submarine cables primary for their own use, traditional ECS/ECN providers still play a key role on the transmission of data for other CAPs, connecting areas where deploying submarine cables by a large CAP may not be economically profitable. Moreover, by primarily interconnecting their data centres and regional points-of-presence (PoPs) to data centres, large CAPs' investments have limited impact on the global network resilience.

Many large CAPs also provide internet relay services, which are used to ensure confidentiality by encrypting the data traffic directly on the users' devices or in the users' domain. The report analyses the potential impact on internet access providers. Depending on the user uptake, these services deserve to be monitored, given their impact on traffic flow, on the utilisation of an internet access providers' current interconnections, and, as a consequence, on the decentralised approach of the internet architecture.

Furthermore, BEREC is aware of some potential issues which deserve to be further analysed to evaluate their impact on the ECS markets. Indeed, recent technological developments and specific services provided by large CAPs (and in particular by OS providers) can sometimes restrict ECN/ECS providers' ability to correctly give access to services or to the network itself. Typical examples include the access to 5G slicing functionalities or other restrictions to the provision of the slices, the potential implications of provider-specific solutions for standardised services (e.g. RCS), as well as the difficulties that some MVNOs and smaller mobile operators seem to face in setting up some functionalities of the devices (e.g. APN-related services, VoLTE, VoWiFi) or in configuring the network profile when eSIMs are used.

To sum up, BEREC's analysis highlights how large CAPs insource what was formerly purchased from traditional ECN/ECS providers to a large degree. Indeed, large CAPs have deployed their own physical infrastructure, such as CDNs and data centres, as well as network infrastructure, such as submarine cables. By building their own large autonomous systems, they rely to a significantly less extent, or not at all, on long-distance transit provided by ECN/ECS operators.

[4] BoR (23) 214, Draft BEREC Report on the general authorization and related frameworks for international submarine connectivity, 07.12.2023, see: https://www.berec.europa.eu/en/document-categories/berec/reports/draft-berec-report-on-the-general-authorization-and-related-frameworks-for-international-submarine-connectivity

The relations between large CAPs and ECS/ECN operators can take several forms: i) CAPs and ECS/ECN operators offer complementary services, which mutually increase each other's demand (e.g. operators providing broadband internet access services and CAPs provide content and applications; the devices and OS by large CAPs being sold together with an operator's bundle offer; set-top boxes integrating both access to the internet and to Over-The-Top services or to voice assistants), and ii) several cooperation partnerships between ECS providers and CAPs can be observed in several countries. However, these actors are also iii) direct competitors, as it is the case for e.g. voice and messages services, video-streaming content platforms vs. linear television and IPTV, cloud service provision, CDNs, submarine cables, as well as for access networks such as LEO satellites, 5G private networks for businesses, and, in some non-European countries, fibre networks.

This report highlights several issues which can raise some challenges in the context of ECS/ECN regulation, and which could be further investigated by BEREC in the future. In order to carry out evidence and fact-based analyses, BEREC stresses the need to collect relevant data from the actors who can have an impact on the ECS/ECN markets which are regulated. The European Electronic Communications Code (EECC) revision provides an opportunity to adapt the regulatory framework and ensure that the current or potential issues can be correctly tackled.

1. Introduction

This report builds on BEREC Report on the Internet Ecosystem[5] and gives an overview of the impact of large CAPs on the markets for ECN and ECS in Europe. It presents their strategies and business models, the market dynamics, as well as CAPs' relations with traditional ECN/ECS providers in terms of competition, cooperation and interdependence. Furthermore, it focuses on three case studies where significant investments by large CAPs are taking place: CDNs, submarine cables and internet relay services.

The report is organised as follows: Chapter 2 provides a general overview of large CAPs' investments in connectivity and cloud infrastructure and their footprint in the European Economic Area (EEA). Chapter 3 summarises the main relations and dynamics between large CAPs and ECS/ECN providers, highlighting specific examples in which they are competing, cooperating and/or are strongly interdependent. Chapters 4, 5 and 6 provide a more in-depth analysis of CDNs, submarine cables, and internet relay services[6], respectively. After giving a brief description of the services involved, these three case studies focus on the business models, the market dynamics and the interactions among the involved stakeholders. Chapter 7 presents some cases where ECS/ECN providers' ability to provide access to the network

[5] BoR (22) 167, BEREC Report on the Internet Ecosystem, 12.12.2022, see: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-internet-ecosystem.

[6] Services providing enhanced privacy features like tracking prevention (e.g. regarding IP-Addresses and DNS) or prevention of precise location determination. Such services include e.g. Apple iCloud Private Relay, Google One VPN or Microsoft Edge Secure Network

and/or to some functionalities and technologies may be affected by OS providers. Chapter 8 presents the main findings of the report, and the lines for future work to be developed by BEREC are described in chapter 9. Annex 1 includes the evolution of voice and SMS from 2005 until 2022.

For this report BEREC circulated a detailed questionnaire to nine major CAPs (Akamai, Amazon, Apple, Cloudflare, Dazn, Google, Meta, Microsoft and Netflix), who responded between 17 July and 8 September 2023. Most of the answers were classified as confidential and therefore the figures presented in this report give a global, aggregated overview.

The questionnaire was sent on the basis of Article 20(1) of the EECC, according to which national regulatory authorities (NRAs) and BEREC have the power to require undertakings who provide ECN and ECS, associated facilities, associated services, or who are active in closely related sectors, to submit information concerning such networks and services. Given the importance of providing a sound and evidence-based analysis of the evolution of ECS and ECN markets, BEREC stresses the need to gather data on relevant services and networks provided by different types of actors.

Furthermore, in order to gather relevant feedback and insights, BEREC organised, a virtual workshop on 21 September 2023 focusing on international submarine connectivity in the European Union[7], where private stakeholders (both traditional ECN/ECS providers and large CAPs), as well as the European Commission, shared their views on the current state of play of the international submarine connectivity business in the EU. The workshop focused on the dynamics following the entry of new actors, the challenges faced and the expectations regarding the evolution of the European and national regulatory framework, institutional organisation and public policies in this area. Moreover, BEREC also organised internal workshops to gather specific insights from selected stakeholders on a selection of topics addressed in this report.

It should be noted that BEREC is addressing closely related topics under several reports.

First of all, BEREC is currently assessing the state of the IP interconnection market and in particular the current trends and the developments in the market, the relations between different parties, use of paid peering and CDNs under the "BEREC Report on the IP interconnection ecosystem"[8]. The discussion on the CAPs' contribution to network investments is therefore not addressed in the current report.

[7] BEREC Workshop on international submarine connectivity in the EU, 21.09.21, see: https://www.berec.europa.eu/en/events/berec-events-2023/berec-workshop-on-international-submarine-connectivity-in-the-eu.

[8] BoR (23) 210, BEREC Work Programme 2024, 07.12.2023, see section 2.4: https://www.berec.europa.eu/en/document-categories/berec/berec-strategies-and-work-programmes/berec-work-programme-2024

Moreover, BEREC has recently published an “External study on the trends and policy/regulatory challenges of cloudification, virtualisation and softwarisation in telecommunications”[9], as well as the “Draft BEREC report on cloud services and edge computing”[10], which is currently under public consultation.

Finally, BEREC has also published a “Report on the general authorisation and related frameworks for international submarine connectivity”[11] which aims to clarify the general authorisation and related frameworks applicable to international submarine connectivity and to identify possible solutions to promote investment in this sector[12].

Regarding the terminology used, it should be noted that large CAPs may provide a diverse range of services, including content aggregation, search engines, messaging applications, entertainment and e-commerce, catering to the interests and needs of media companies, content creators, and individual users. Along this report, depending on their core activity, CAPs may also be referred to as edge providers, operating systems (OS) providers, cloud providers, or hyperscalers. For the purposes of this report, “hyperscalers” mean very large cloud service providers, which use (make or make buy) large-scale data centres widely geographically available. They are able to deliver massive amounts of computing power, resources and infrastructure for the provision of a large portfolio of services, ensuring seamless scalability. Moreover, while traditional ECN/ECS providers can also provide content-related services, they are not referred to as “CAPs” or “(large) CAPs” for the purpose of this report.

It should also be noted that here the term “market” – especially when referring to digital services/networks – is used in a general way, and not as the result of the market definition as carried out in ECS *ex ante* regulation or in *ex post* competition law.

[9] BoR (23) 208, External study on the trends and cloudification, virtualization, and softwarization in telecommunications, 07.12.2023, see: https://www.berec.europa.eu/en/document-categories/berec/reports/external-study-on-the-trends-and-cloudification-virtualization-and-softwarization-in-telecommunications

[10] BoR (23) 210, BEREC Work Programme 2024, 07.12.2023, see section 1.6: https://www.berec.europa.eu/en/document-categories/berec/berec-strategies-and-work-programmes/berec-work-programme-2024

[11] BoR (23) 214, Draft BEREC Report on the general authorization and related frameworks for international submarine connectivity, 07.12.2023, see: https://www.berec.europa.eu/en/document-categories/berec/reports/draft-berec-report-on-the-general-authorization-and-related-frameworks-for-international-submarine-connectivity

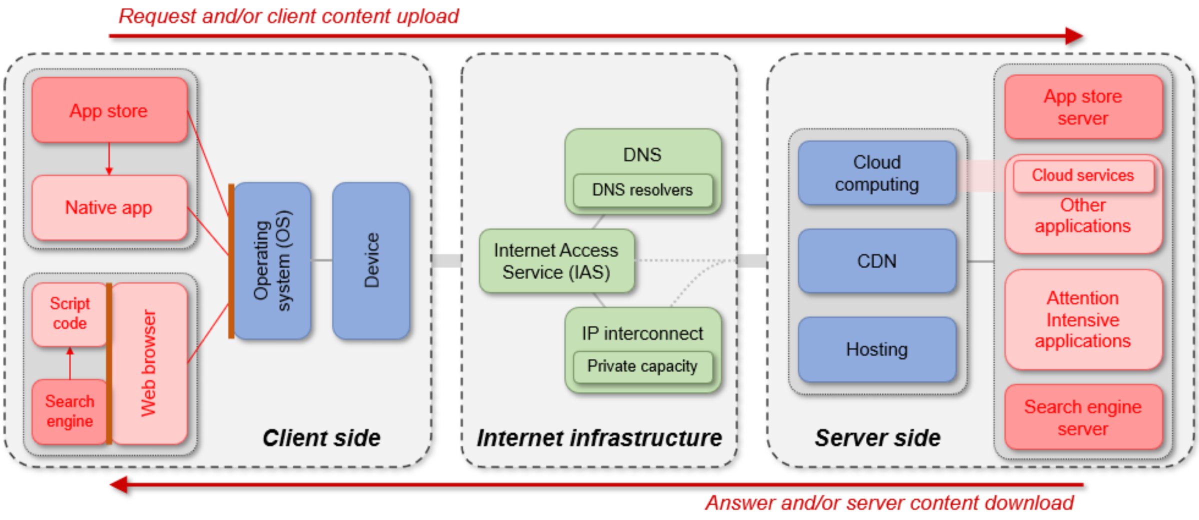
[12] BEREC organised a workshop on secure and reliable connectivity from LEO satellite fleets on 13 April 2023, see: https://www.berec.europa.eu/en/events/berec-events-2023/berec-workshop-on-secure-and-reliable-connectivity-from-leo-satellite-fleets

2. Overview of large CAPS investments

2.1. CAPs' investments in internet infrastructure in the EEA

Several elements of the internet ecosystem are involved to bring content and/or service to the end-users. Based on the work done by BEREC[13], Figure 1 shows the elements in the internet ecosystem including the client side (e.g. device, OS and applications), the internet infrastructure (network elements supporting the communication between the client and the server side), and the server side (all elements used by CAPs to provide the content and/or service).

Figure 1. The elements in the internet ecosystem



***Legend**: **Green** boxes represent the connectivity segments/services; **Blue** boxes represent the hardware and software from the device or cloud server; **Red** boxes represent the client-server application that is being used*

Source: BEREC Report on the Internet Ecosystem[14]

Large CAPs have traditionally provided content and/or services on the client and server sides of the internet ecosystem and did not generally deploy their own infrastructure. However, in recent years, large CAPs have increasingly invested in network infrastructure and have been providing additional services closely related to ECN and ECS, or directly qualifying as such. They have deployed their own physical infrastructure such as CDNs and data centres, as well

[13] BoR (22) 167, BEREC Report on the Internet Ecosystem, 12.12.2022, see:https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-internet-ecosystem.

[14] BoR (22) 167, BEREC Report on the Internet Ecosystem, 12.12.2022, see: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-internet-ecosystem

as submarine cables and satellites constellations[15] and have thus insourced many services which were previously provided by ECN/ECS operators.

Among other reasons, the decision to deploy their own dedicated network infrastructures appears to be mainly driven by the increasing demand of their services and the related growth of data transmission that requires higher bandwidth[16], the need to interconnect their data centres worldwide[17], and the will to better control the provision of the services. For large CAPs, depending on the circumstances, it can be economically reasonable to employ a "make" rather than a "buy" strategy since they operate at a sufficiently large scale. Moreover, CAPs' investment in their own network infrastructure reduces dependency from third-party transit providers' services, as well as provides them with more flexibility to manage their own capacity to upgrade[18] and to manage their bandwidth, according to their specific needs. By building up these infrastructures they can manage and improve the quality of their service and subsequently improve the user experience. Additionally, certain large CAPs provide CDN services to third parties, while others only use CDNS for self-provision (see Chapters 4 and 5).

Regarding data centres, the Subtel report[19] mentions that these infrastructures are becoming essential components also to the submarine telecom ecosystem, due to the proximity of the data centres to the cable landing stations, which optimizes interconnection and network services, minimizes latency and simplifies the infrastructure.

According to Analysys Mason[20], CAPs worldwide have been making significant investments in infrastructure, in particular in three main domains: hosting[21] (i.e. data centres and cloud), transport (i.e. submarine and terrestrial cables) and delivery (i.e. peering and caching) (see Figure 2). Hosting appears to be the most significant area of CAPs' investment in infrastructure, and represented for the period 2018-2021almost 94% of the total investment in

[15] For example, Amazon Project Kuiper, see: https://www.aboutamazon.com/what-we-do/devices-services/project-kuiper.

[16] Since 2019 demand for international internet bandwidth has tripled to more than 3,800 terabits per second, estimates TeleGeography. The boom in data-hungry artificial intelligence may strengthen this trend - The Economist, Big Tech and geopolitics are reshaping the internet's plumbing, 20th December 2023.

[17] According to Sandvine, almost 48% of all global data traffic (including fixed and mobile networks) in 2022 can be attributed to the six major tech players, namely Meta (Facebook, Instagram, WhatsApp), Google (YouTube), Apple, Amazon (AWS, Amazon Prime), Microsoft (MS Office, Xbox) and Netflix. Sandvine, The Global Internet Phenomena Report, 2023, see: https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2023/reports/Sandvine%20GIPR%202023.pdf

[18] BoR (17) 184, BEREC Report on IP-Interconnection practices in the Context of Net Neutrality, 05.10.2017, see: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-ip-interconnection-practices-in-the-context-of-net-neutrality

[19] Subtel Forum Submarine Telecoms Industry Report, Industry Report 2023-2024, see: https://subtelforum.com/industry-report/.

[20] Analysys Mason, The Impact of tech companies' network investment on the economics of broadband ISPs, see: https://www.analysysmason.com/contentassets/b891ca583e084468baa0b829ced38799/main-report---infra-investment-2022.pdf.

[21] BoR (22) 167, BEREC Report on the Internet Ecosystem, 12.12.2022, see: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-internet-ecosystem . Here hosting is considered to be on the server side.

the three domains. A large share of this investment relates to self-built hyperscale data centres. In order to connect these data centres to each other and to the delivery networks, investments in long-distance networks has also increased. Moreover, the need to move and host content closer to end-users to improve the quality of experience while managing cost efficiency, has become more critical. In this context, CAPs' investment in transport infrastructure has also grown. CAPs also continue to develop delivery networks to bring services closer to end-users, through border gateways in Internet Exchange Points (IXPs), private peering facilities, and caches inside ISP networks. However, until now CAPs have not yet invested in access networks in the EU.

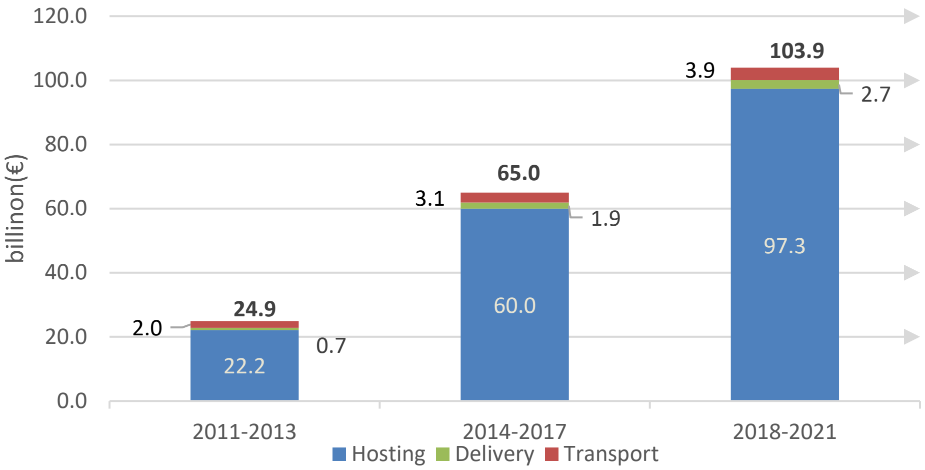
According to Analysys Mason, the total spent on internet infrastructure (i.e. hosting, transport and delivery) reached around 751 billion euros for the period 2011–2021 worldwide, in detail:

- 75 billion euros for the period 2011-2013;
- 260 billion euros for the period 2014-2017; and
- 416 billion euros for the period 2018-2021.

However, according to STRAND Consult[22] the total internet infrastructure investments made by the CAPs only represent approximately 1% of their global revenue.

Additionally, Analysys Mason also presents the average annual investment made by CAPS on internet infrastructure (Figure 2).

Figure 2. CAPs average investment in infrastructure by period.



Source: Adapted from Analysis-Mason, 2022, p. 10

[22] Fact Check on Analysys Mason's Claims on Big Tech Investments and Arguments Against Broadband Cost Recovery, STRAND Consult, May 2023

Specifically in Europe, according to Analysys Mason[23], the average annual investment on internet infrastructure (i.e. in hosting, transport and delivery) in Europe was around:

- 8 billion euros for the period 2011-2013;
- 15 billion euros for the period 2014-2017; and
- 21 billion euros for the period 2018-2021.

This represents around 170 billion euros for the period 2011-2021, which represents about 23% of their global investment.

In 2022, according to the European Commission's 2022 EU Industrial R&D Investments scoreboard[24], seven of the largest CAPs[25] invested 70,5 billion euros (CAPEX) on infrastructure worldwide (data centres, CDNs, submarine cables, terrestrial and satellite networks) mainly to support the delivery of their own services and bringing content closer to end-users. While CAPEX does not solely represent investment in infrastructure, it can provide insights of the magnitude and scale of investments.

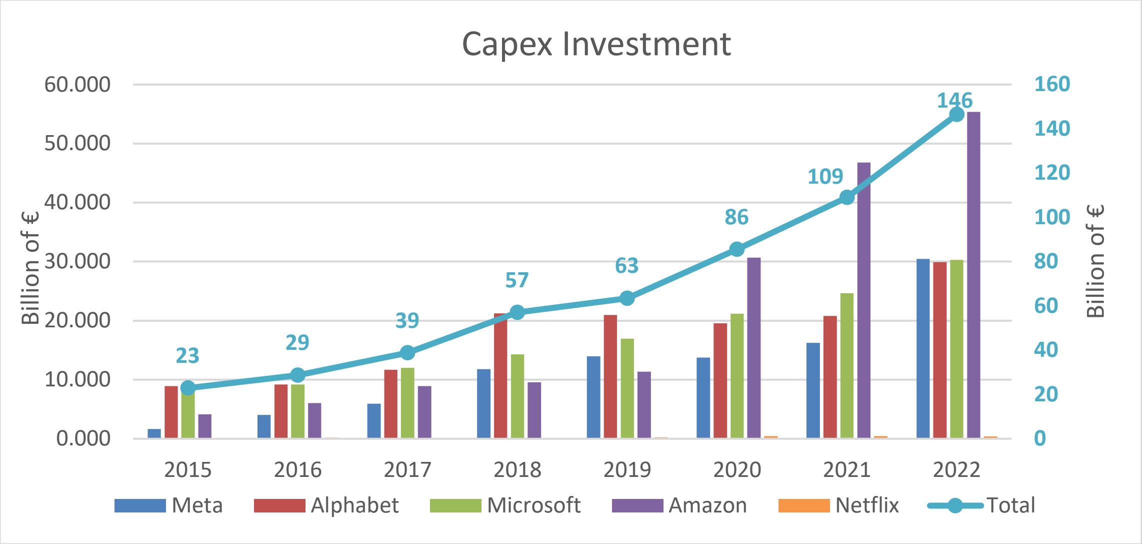
Collectively, the five largest CAPs invested a total of 146,3 billion euros in capital expenditures in 2022 globally, which compares with a total of 22,5 billion euros in 2015, that represents a Compound Annual Growth Rate (CAGR) of 29% per year. Since 2019, these investments have more than doubled.

[23] Europe infrastructure investment report, see: https://www.analysysmason.com/contentassets/b891ca583e084468baa0b829ced38799/europe-infographic---infra-investment-2022.pdf

[24] The 2022 EU Industrial R&D Investment Scoreboard, 13.12.2022, see: https://iri.jrc.ec.europa.eu/scoreboard/2022-eu-industrial-rd-investment-scoreboard

[25] Apple, Google, Meta, Microsoft, Netflix, Spotify and Twitter.

Figure 3. Larger CAPs investment in Capex, 2015-2022



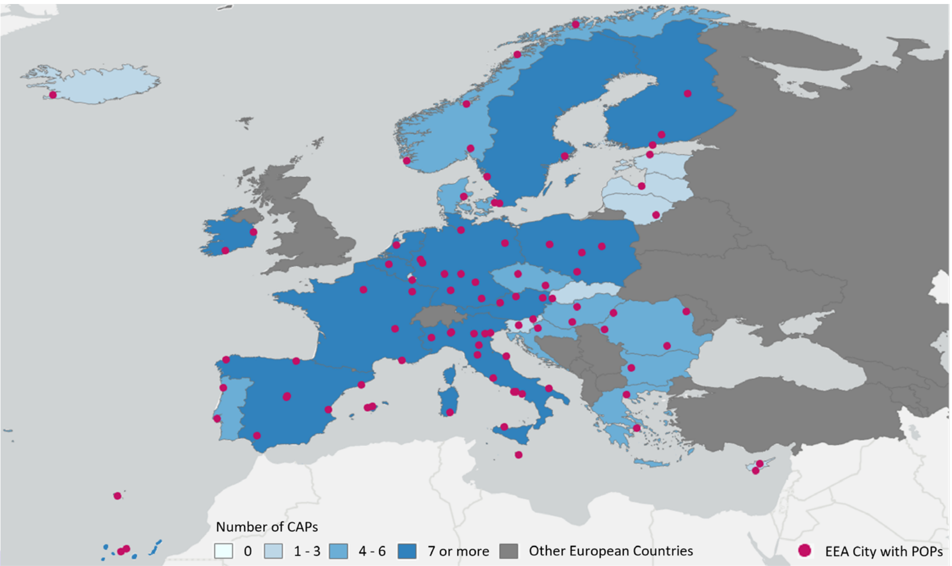
Source: BEREC, based on company's financial results reports

2.2. CAPs' points of presence in the EEA

Large CAPs' footprint can be represented by their PoPs. Via its questionnaire, BEREC collected data concerning the PoPs of nine large CAPs within the EEA.

For the purposes of this report, a PoP is defined as a physical location or facility that houses network equipment (e.g. servers and routers) to interconnect with other networks.

Figure 4. Nine major CAPs' presence and PoPs in EEA countries.



Source: BEREC

Within the EEA, Figure 4 shows both the number of CAPs (who responded to the BEREC questionnaire) by country and the cities/metropolitan areas where these CAPs have at least one PoP.

It is possible to conclude that these CAPs are present throughout all EEA countries (with the only exception of Lichtenstein) and that there are 90 cities where CAPs have at least one PoP. The number of cities per country in which the nine CAPs have PoPs varies greatly: in some countries the CAPs are only present in one city (e.g. Belgium) while in others they are present in many cities (e.g. 16 cities in Italy[26]).

The data gathered by BEREC also show that:

- In 60% of the EEA countries the CAPs are present in more than one city in the same country;
- In nearly 20% of the cities (10 of which are capital cities) almost all the CAPS have a PoP;
- In almost 50% of the cities only one CAP is present[27].

This heterogeneous presence of CAP in each country/city seems to indicate that, although the approach followed by each CAP varies, presence in EEA countries seems to represent an important part of CAPs' strategy.

2.3. CAPs' investments in cloud infrastructures

Cloud infrastructure, jointly with hosting and CDNs, are the elements of the internet ecosystem[28] where server computers are run, delivering CAPs' content and applications.

The term "cloud computing service"[29] encompasses a set of infrastructures and services which enable on-demand scalable access to a shared pool of (physical and virtual) computing resources and include, primarily, storage (data servers, data centres, hosting of data, content, applications), CPU resources, networking, runtime software, applications, and software for data analysis.[30] Cloud infrastructures and services are an essential building block of the global

[26] Please note that PoPs within the same metropolitan area or city are counted as one.

[27] Cities with only one CAP do not appear in the map to respect the confidentiality of the responses received.

[28] For a more detailed analysis: BoR (22) 167, BEREC Report on the Internet Ecosystem, 12-12-2022, see: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-internet-ecosystem.

[29] "Cloud computing service means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations", Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, 27.12.2022, see: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1706174547788

[30] The cloud services have recently been investigated by regulatory and competition authorities in many studies and reports amongst which are the following: ACM, Market Study Cloud Services, 2021, see: https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf; Autorité de la Concurrence,

strategy of large CAPs to expand capacity and connectivity for the flourishing of data-driven and artificial intelligence (AI)-enabled services. A developed cloud-based infrastructure eases the integration of cloud and CDN services in CAPs' offers, and provides their clients with a collection of different tools.[31] There exist different types of cloud services according to the service (IaaS, PaaS, SaaS)[32] and the deployment models (public, private, community, hybrid).[33]

In general terms, a global cloud infrastructure is made up of regions (broad geographical areas which can be broader than a continent, i.e. Eurasia) and crucial PoPs[34], which are called Availability Zones (AZs). These AZs are clusters of data centres located in strategic areas having independent power, cooling and networking infrastructure, as well as a given level of resiliency in case of outages.[35] The main three global cloud players – Amazon (AWS), Google (Google Cloud) and Microsoft (Azure) – have data centres and storage hubs in almost every region of Europe.

Opinion 23-A-08 of 29 June 2023 on competition in the cloud sector, see: https://www.autoritedelaconcurrence.fr/sites/default/files/attachments/2023-09/23a08_EN.pdf; Ofcom, Cloud services market study, 05.10.2023, see: https://www.ofcom.org.uk/__data/assets/pdf_file/0027/269127/Cloud-services-market-study-final-report.pdf; BEREC report on Cloud Services and Edge Computing, to be approved in 2024. BoR (23) 210, BEREC Work Programme 2024, 07.12.2023, see: https://www.berec.europa.eu/en/document-categories/berec/berec-strategies-and-work-programmes/berec-work-programme-2024

[31] Amazon Cloudfront, see: https://aws.amazon.com/cloudfront/; Google Cloud CDN overview, see: https://cloud.google.com/cdn/docs/overview; Azure CDN, see: https://azure.microsoft.com/en-us/products/cdn

[32] Infrastructure as a Service (IaaS): The IaaS provides customers with network, storage, processing, and other computing infrastructure resources. The customer doesn't control or manage the infrastructure but has control over the applications, operating systems, and programming frameworks. Platform as a Service (PaaS): The PaaS enable customers to adopt applications which are developed using specified framework, programming language, and tools onto a cloud infrastructure. The customer doesn't control or manage over PaaS but has control over the deployed applications. Software as a Service (SaaS): the SaaS allows customers to access applications running on a cloud infrastructure from several end-user devices. Here, the SaaS service enable users to have control over a limited number of user-specific applications.

[33] Public cloud: infrastructure that supports all users who want to make use of a computing resource, such as hardware (OS, CPU, memory, storage) or software (application server, database) on a subscription basis. Private cloud: typically infrastructure used by a single organization, managed by the organization itself to support various user groups, or it could be managed by a service provider that takes care of it either on-site or off-site. Hybrid cloud: when interconnected private and public cloud infrastructure is used. Community cloud: multiple organizations sharing computing resources that are part of a community; examples include universities or state sharing computing resources. BEREC report on Cloud Services and Edge Computing, to be approved in 2024. BoR (23) 210, BEREC Work Programme 2024, 07.12.2023, see: https://www.berec.europa.eu/en/document-categories/berec/berec-strategies-and-work-programmes/berec-work-programme-2024

[34] Even if the network also includes network PoPs and recovery PoPs.

[35] What are availability zones? See: https://learn.microsoft.com/en-us/azure/reliability/availability-zones-overview?tabs=azure-cli; Regions and zones, see: https://cloud.google.com/compute/docs/regions-zones; What is Amazon ElastiCache for Memcached? See: https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/RegionsAndAZs.html

The market for cloud services is highly concentrated and the three biggest players accounted for 66% of the market[36] globally[37] and 72% of the market in Europe[38] in 2023.

Amazon is a vertically integrated large CAP whose cloud and edge infrastructures allow to offer to potential customers an array of about 200 different cloud services. Amazon's cloud and edge network is organised in macro-categories (AWS Regions)[39]. Google has a global cloud network, which in Europe enlists 12 regions: it is present in 10 European countries, out of which 8 are EU Member States. Currently, in Europe, Google offers 14 macro categories of cloud and cloud related services[40], some of which have already a global print, therefore are available independently from the location. Google also offers a set of interconnection tools and capabilities,[41] which can be grouped in two clusters: Google Interconnect and Direct peering.[42] Microsoft offers an array of cloud services that are grouped into 21 categories.[43] On the same foot, Microsoft also has a global cloud network subdivided into regions (about 60),[44] AZs and other PoPs. Cloud capabilities are connected through a space infrastructure for providing failover capabilities or preventing disruption by natural disasters, etc.[45]

On the other hand, the European providers' market share is decreasing. The major European cloud providers, SAP and Deutsche Telekom, account each for 2% of the European market[46] and are followed by OVHcloud, Telecom Italia, Orange and other national and regional players. Some ECS providers are also active as cloud providers and as cloud customers for their own operations. A potential driver of their shift towards cloud and edge investment is the

[36] IaaS, PaaS, SaaS, hosted private cloud

[37] Huge Cloud Market Still Growing at 34% Per Year; Amazon, Microsoft & Google Now Account for 65% of the Total, Synergy Research Group, see: https://www.srgresearch.com/articles/huge-cloud-market-is-still-growing-at-34-per-year-amazon-microsoft-and-google-now-account-for-65-of-all-cloud-revenues

[38] European Cloud Providers Continue to Grow but Still Lose Market Share, see: https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share

[39] AWS Global Infrastructure, see: https://aws.amazon.com/about-aws/global-infrastructure/?nc1=h_ls. A Region in AWS network topology is not a single data centre, but it is a physical location around the world where data centres are clustered. Each group of logical data centre is called Availability zone (AZ). Each AWS Region "consists of a minimum of three, isolated and physically separated AZs within a geographic area". Each AZ has independent power, cooling and physical security is connected via redundant, ultra-low latency networks (Regions and Availability Zones, see: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/?nc1=h_ls).

[40] 1 Compute, 2 Storage and databases, 3 Big data and ML, 4 Developer tools, 5 Identity and security, 6 Healthcare and life sciences, 7 API management, 8 Integration services, 9 Media and gaming, 10 Operations, 11 Financial Services, 12 Analytics, 13 Compliance, 14 AI/ML.

[41] *Dedicated Interconnect* provides a direct physical connection between the client on-premises network and the Google network. *Partner Interconnect* provides connectivity between the client's on-premises and VPC networks through a supported service provider. *Cross-Cloud Interconnect* provides a direct physical connection between the client network in another cloud and the Google network.

[42] Direct Peering overview, Network Connectivity, Google Cloud, see: https://cloud.google.com/network-connectivity/docs/direct-peering; also the difference between the two clusters in Choosing a Network Connectivity product, Google Cloud, see: https://cloud.google.com/network-connectivity/docs/how-to/choose-product#dp-compare

[43] Azure products, see: https://azure.microsoft.com/en-us/products

[44] Azure global infrastructure experience, see: https://datacenters.microsoft.com/globe/explore

[45]Azure space experience, Azure global infrastructure experience, see: https://datacenters.microsoft.com/globe/explore/space

[46] European Cloud Providers Continue to Grow but Still Lose Market Share, Synergy Research Group, see: https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share

steady growth of information flows produced by VHCN networks and the business value it can generate across a variety of industry applications[47]. Another factor is the cloudification of network functions, as in the case of stand-alone 5G networks, which employ a native cloudified core network and the trend towards the virtualization of the radio access network part.

From 2022 to 2026, the global public cloud services market revenues are expected to grow at a CAGR of 19.8%, which predictably will increase the demand for hyperscale data centres[48]. This growth of cloud computing and the expected future developments towards edge computing attract partnerships and enable synergies with the electronic communications[49]: i) Connectivity among data centres and between the data centres and the end-users. In order to use scalable cloud services, customers need to access a network and the bidirectional transit of data (to and from the cloud provider) may rely on the public internet or on a private connection; ii) the supply of bundled and integrated ECN/ECS and IT services with cloud; iii) ECN/ECS evolution towards network cloudification[50] and iv) the provision of services based on Network-as-a-Service solutions.

3. Dynamics between large CAPs and ECS/ECN operators

Relations and dynamics between CAPs and ECS/ECN operators can be of different kinds: competition, cooperation and interdependence.

Many ECS/ECN operators are increasingly embracing virtual and cloud-native network architectures[51] and sometimes enlarging their portfolio to also become digital service providers. CAPs, on the other hand, are striving to move their services closer to the end-user, leveraging their wide IT services portfolio. These developments are driving both the competition and cooperation dynamics between CAPs and ECS/ECN operators.[52]

[47] BoR (23) 208, External study on the trends and cloudification, virtualization, and softwarization in telecommunications, 07-12-2023, see: https://www.berec.europa.eu/en/document-categories/berec/reports/external-study-on-the-trends-and-cloudification-virtualization-and-softwarization-in-telecommunications

[48] IDC world wide world cloud revenue forecast, 2022; 2023 Global Data Centre Outlook, p. 12.

[49] This is further analysed under the Draft BEREC report on Cloud Services and Edge Computing, to be approved in 2024. BoR (23) 210, BEREC Work Programme 2024, 07.12.2023, see: https://www.berec.europa.eu/en/document-categories/berec/berec-strategies-and-work-programmes/berec-work-programme-2024

[50] BoR (23) 208, External study on the trends and cloudification, virtualization, and softwarization in telecommunications, 07.12.2023, see: https://www.berec.europa.eu/en/document-categories/berec/reports/external-study-on-the-trends-and-cloudification-virtualization-and-softwarization-in-telecommunications

[51] BoR (23) 208, External study on the trends and cloudification, virtualization, and softwarization in telecommunications, 07.12.2023, see: https://www.berec.europa.eu/en/document-categories/berec/reports/external-study-on-the-trends-and-cloudification-virtualization-and-softwarization-in-telecommunications

[52] The relations between CAPs and internet access service (IAS) providers in the IP interconnection market (including the bargaining situation between the two) is not analysed here but will be the focus the BEREC Report on the IP Interconnection ecosystem, to be approved in 2024. BoR (23) 210, BEREC Work Programme

3.1. Complementary services and interdependence

CAPs and telecommunications operators provide different and often complementary services along the internet value chain, and thus mutually enable and increase demand for each other services. On the one hand, ECS/ECN operators typically provide connectivity, while CAPs provide content and applications, and may provide other elements in the Internet value chain, such as operating systems (OS), app stores and devices[53]. Since no online content and applications could be consumed without connectivity, and no connectivity would be required without any online content and applications, there is an interdependence between CAPs and ECS/ECN operators.

In several cases, inputs are directly supplied from ECS/ECN operators to CAPs or the other way around. For instance, CAPs may buy transport services from operators. If CAPs operate their own CDNs, they are less reliant on transit services, but still need telecommunications operators for the termination of the traffic to the end-users.

ISPs, for their part, benefit from the delivery of CAPs services and products through increased demand for connectivity and bandwidth that they can monetise to end-users. Networks with increased capacities also allow for innovations and new forms of content, which in turn may increase the take-up of enhanced networks.

As far as devices and OS are concerned, we observe similar dynamics when it comes to mobile phones, set-top boxes or virtual assistants. In their offers, ISPs use or integrate devices developed by some CAPs which may include applications or software.

For mobile phones, some of the devices and/or OS are provided by large platforms, in particular Apple's iPhone and iOS and Google's Android. ECS/ECN operators usually provide devices to their customers together with a contract for voice, SMS, and internet access or as stand-alone. For example, in order to be able to unrestrictedly use iPhones in the network with extended functionalities such as eSIM or VoLTE, telecommunications operators need a contract with Apple and some smaller operators find it difficult to conclude such contracts (see chapter 7). Moreover, ECS/ECN operators have the option of pre-installing apps to personalise the devices that their users acquire through them, for example by installing customer self-care apps. A customer self-care app enables the customer to make settings for his account and to view the billing, for example. In addition to their own apps, there is also the possibility of pre-installing third-party apps (for example, marketplaces such as Amazon), which might be paid for by the app providers.

2024, 07.12.2023, see: https://www.berec.europa.eu/en/document-categories/berec/berec-strategies-and-work-programmes/berec-work-programme-2024

[53] BoR (22) 167, BEREC Report on the Internet Ecosystem, 12.12.2022, see: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-internet-ecosystem

In the context of the telecommunications bundled offers, in some EU countries users often get two devices with their internet subscription[54]: the router, which integrates internet connection access and home router functions (modem/ONT, WiFi, firewall, etc.), and a set-top box that gives access to Over-The-Top (OTT) services (TV, VoD/streaming, OTT offers, etc.). Some set-top boxes can include either Android/Apple TV or some components from Android, with software overlays made or controlled by the ISP itself. Therefore, ISPs had to ensure less investment in the firmware for this product, and the CAP benefits from the access to a new user base.

A similar situation can be observed for voice assistants, which have recently been integrated in some set-top boxes (Amazon Alexa or Google Assistant). It should be noted that Orange and Deutsche Telekom tried to develop their own vocal assistant, Djingo, which was launched in France in November 2019[55] but stopped being commercialised nearly a year after[56]. In September 2022, Orange integrated Amazon voice assistant, Alexa, to its set-top box[57]. The market appears to be concentrated around few players[58].

Finally, concerning cloud services, some ECS/ECN operators buy cloud services from CAPs which can go as far as hosting core network functionalities in the cloud. For certain high quality / low latency connectivity services, cloud services may even be integrated in the edge of the telecommunications operators' networks. OpenRAN is another development, where (active) components of the radio access network are no longer provided only by specialised equipment vendors but also e.g. by CAPs acting as large cloud providers. These developments are leading towards cloud-network convergence for the provision of ECN/ECS.[59]

3.2. Areas of competition

The most obvious and direct area of competition between CAPs and ECS/ECN operators is probably for messages and voice services. A BEREC study analysing EU consumers perceptions and behaviour on digital platforms for communication[60] revealed patterns both of

[54] In the EU the Open Internet Regulation grants users the possibility to use the equipment of their choice. Nevertheless, in practice, this choice is limited as the average user have little incentives to buy his/her own terminal equipment.

[55] Orange launches the voice assistant Djingo to make its customers' everyday lives easier, see: https://newsroom.orange.com/orange-launches-the-voice-assistant-djingo-to-make-its-customers-everyday-lives-easier/?lang=en

[56] Orange Will Wind Down Djingo Smart Speaker in Favor of Smart Home and TV Services, see: https://voicebot.ai/2020/10/07/orange-will-wind-down-djingo-smart-speaker-in-favor-of-smart-home-and-tv-services/

[57] Le service vocal de la TV d'Orange s'enrichit avec Alexa, see: https://newsroom.orange.com/tvorange-alexa/?lang=frhttps://newsroom.orange.com/tvorange-alexa/?lang=fr

[58] See: https://www.statista.com/statistics/792604/worldwide-smart-speaker-market-share/

[59] BoR (24) 52 Draft BEREC Report on Cloud and Edge Computing Services: https://berec.europa.eu/en/document-categories/berec/reports/draft-berec-report-on-cloud-and-edge-computing-services

[60] BoR (21) 89, Analysing EU consumer perceptions and behaviour on digital platforms for communication. Analysis report, 10-06-2021, see: https://www.berec.europa.eu/en/document-categories/berec/reports/analysing-eu-consumer-perceptions-and-behaviour-on-digital-platforms-for-communication-analysis-report

complementarity and substitution when it comes to consumer switching between digital and traditional electronic means of communication.

While the number of SMS decreased significantly with the increasing usage of number-independent interpersonal communication services provided by CAPs, number-based voice services do not seem to be affected. Figure 12 in Annex 1 presents the aggregated volumes of voice minutes and SMS from 2009 to 2022 in 19 European countries, while Figure 13 and Figure 14 show the volume of voice minutes and SMS from 2005 to 2022 in 22 European countries. All graphs present the evolution compared to 2012. The graphs show a similar trend in most of these countries: between 2005 and 2022, the volume of call minutes did not vary significantly[61]. However, the volume of SMS first increased during the 2000s, then decreased during the 2010s.

Also, video-streaming content offered by CAPs (e.g., Netflix, Amazon Prime Video, Disney+) is increasingly competing with linear television as well as with cable TV / IPTV-offers from telecommunications operators, which has often led the latter to integrate CAPs SVoD[62] platforms into their own TV environment or develop their own catch-up and on demand TV services.

Another area of (retail) competition is the provision of cloud services and business services.[63] Since hyperscalers usually have much larger cloud capacities than ECS/ECN operators and can make use of high economies of scale and scope as well as of network effects, the offers proposed by ECS/ECN operators are usually not competitive as they can't provide the same portfolio of products and economic ingress advantages (e.g. credits or volume discounts). When providing cloud services, ECS/ECN operators are often offering solutions specialised in data sovereignty and security in order to differentiate themselves from the hyperscalers (although some ECS/ECN operators may also offer solutions aiming at data sovereignty alongside with hyperscalers)[64]. Several ECS/ECN operators also resell large cloud providers' products in a bundle with their own services benefiting from the commercial relation built over the years with business customers.[65]

[61] With the exception of the pandemic period, when most countries temporarily experienced an increase.

[62] Subscription Video on Demand

[63] BEREC report on Cloud Services and Edge Computing, to be approved in 2024. BoR (22) 193, BEREC Work Programme 2023, 12.12.2022, see: https://www.berec.europa.eu/en/document-categories/berec/berec-strategies-and-work-programmes/berec-work-programme-2023

[64] For example, in France, some telecommunication operators conducted partnership with industrial actors to provide cloud services offers meeting the requirements of the SecNumCloud qualification, elaborated by the French national agency for security of information systems, ANSSI (see: https://www.ssi.gouv.fr/secnumcloud-pour-les-fournisseurs-de-services-cloud/). This is the case of Bouygues Telecom, who partnered with Docaposte, Dassault Systèmes and la Banque des territoires to create Numspot (see: https://numspot.com/). Orange and Capgemini also formed a joint venture named "Bleu" to provide cloud services that would meet SecNumCloud qualification, in this case providing Microsoft Azure services (see: https://www.capgemini.com/news/press-releases/capgemini-and-orange-announce-that-bleu-will-start-engaging-with-customers-by-the-end-of-2022/).

[65] See for example the offer of Téléfonica: https://cloudportal.telefonicatech.com/us/

In the business sector, hyperscalers also offer UCC (Unified Communication and Collaboration) services including voice services (also to national number plans), video conferencing services, chats, collaboration tools, etc. replacing traditional business connectivity services offered by telecommunications operators[66]. Data centres[67] and hosting services are also increasingly provided by firms like Amazon, Google or Microsoft (see Chapter 2).

Access networks and internet or voice access services are largely provided by ECS/ECN operators, although some competition from CAPs is emerging, such as the LEO satellite networks e.g. by Amazon (Project Kuiper)[68] or the 5G private networks for businesses e.g. also by Amazon[69]. However, these services are not yet taken up on a broad scale: the take-up of 5G private networks services is still low and LEO satellite networks are mainly used in very rural areas with poor fixed and mobile coverage. Some CAPs also started to deploy their own fibre access networks, e.g. Google Fibre in the USA[70], and Sky Italia uses access to fibre networks to provide retail internet and bundled services in Italy. Such cases are however rare and access networks remain difficult to replicate due to economies of scale and large sunk costs.

In the backbone and on transit routes, significantly more entry by CAPs can be observed, with CAPs rolling out their own CDNs (see Chapter 4) and their own infrastructure including submarine cables (see Chapter 5). While such a rollout competes directly with transit providers, access providers can actually benefit from these developments since the content and the handover of traffic will be closer to their retail customers.

The online advertising markets on the other hand are clearly dominated by large CAPs.[71] Some internet relay services (see Chapter 6) provided by large CAPs could make it more difficult for ECS providers to provide personalised advertising since users' IP addresses and other information are encrypted. As a reaction, some ECS providers founded a joint venture[72]

[66] BoR (22) 184, External Study on Communication Services for Businesses in Europe: Status Quo and Future Trends, 12-12-2022, see: https://www.berec.europa.eu/en/document-categories/berec/others/external-study-on-communication-services-for-businesses-in-europe-status-quo-and-future-trends

[67] According to the ACM study, data centres contributes significantly to the economies of scale of cloud services, both with regard to the size of one data centre, and with regard to having multiple data centres worldwide.

[68] Project Kuiper is an initiative from Amazon to build a low Earth orbit (LEO) satellite constellation providing broadband service around the world, by means of 3,236 satellites. Amazon announced that they will invest more than 10 billion dollars in Project Kuiper. In July 2020, the US Federal Communications Commission granted Amazon a licence, that requires to deploy and operate at least half of the satellite constellation by July 2026. See: https://www.aboutamazon.com/news/company-news/amazon-receives-fcc-approval-for-project-kuiper-satellite-constellation?ots=1&tag=arstech20-20&linkCode=w50

Everything you need to know about Project Kuiper, Amazon's satellite broadband network, see: https://www.aboutamazon.com/news/innovation-at-amazon/what-is-amazon-project-kuiper

[69] AWS Private 5G, see: https://aws.amazon.com/private5g/

[70] Google fibre, see: https://fibre.google.com/

[71] See for example Statista, Companies with largest share of digital advertising revenue worldwide in 2023, https://www.statista.com/statistics/290629/digital-ad-revenue-share-of-major-ad-selling-companies-worldwide/

[72] Mergers: Commission clears creation of a joint venture by Deutsche Telekom, Orange, Telefónica and Vodafone, see: Mergers: Commission clears creation of a joint venture (europa.eu)

to create Utiq[73], a European AdTech company that delivers a telco-powered consent service, which uses an identifier for advertising purposes which differs from the IP address.

3.3. Cooperation

There are also examples of projects where CAPs and ECS/ECN providers cooperate. This section lists some of them without aiming to provide a complete overview.

First of all, several partnerships between CAPs and ECS/ECN concern cloud services:

- Microsoft conducted partnerships with European telecommunications operators to develop cloud computing services (e.g. Microsoft and Deutsche Telekom announcement in 2020[74]), business-oriented services (e.g. Microsoft and BT announcement in 2021[75]), or AI-based services aiming at transforming customer experience (e.g. Microsoft and Telefonica announcement in 2019[76]).

- Open Gateway[77] is a GSMA[78]-led initiative in the telecommunications sector that seeks to transform the communications networks into platforms. Telecommunications capabilities are deployed through global and standardised APIs designed to provide universal access to operator networks for developers. Launched with the support of 21 mobile network operators, this initiative will help developers and cloud providers enhance and deploy services more quickly across operator networks via single points of access to the world’s largest connectivity platform. These APIs will be available through the digital environments of cloud providers, such as AWS, Microsoft Azure and Google Cloud.

- In Italy, Google has just built the second cloud region in partnership with Telecom Italia which is intended to provide for faster, more reliable and secure cloud services, as well as to deliver highly available, low-latency application for customers[79].

[73] Towards a trusted and responsible digital world for everyone, see: https://utiq.com/ (previously TrustPID) See: https://www.trustpid.com/

[74] Deutsche Telekom and Microsoft redefine partnership to deliver high-performance cloud computing experiences, see: https://news.microsoft.com/2020/12/09/deutsche-telekom-and-microsoft-redefine-partnership-to-deliver-high-performance-cloud-computing-experiences/

[75] BT and Microsoft announce strategic partnership, see: https://newsroom.bt.com/bt-and-microsoft-announce-strategic-partnership/

[76] Telefónica and Microsoft establish strategic partnership to design the telco of the future, see: https://news.microsoft.com/2019/02/25/telefonica-and-microsoft-establish-strategic-partnership-to-design-the-telco-of-the-future/

[77] Mobile Industry Deploys Open Network APIs and Prepares for New Era of Digital Services and Mobile Apps, see: https://www.gsma.com/newsroom/press-release/gsma-open-gateway/

[78] Global System for Mobile Communications Association.

[79] The first region is in Milan, for this second hub in Turin see Il Sole 24 Ore. Internet e Telecomunicazioni, “Cloud, Google fa il bis con Tim e Intesa nel data centre di Milano”, p. 29, 24 March 2023

Other partnerships concern the deployment of 5G cloud native networks:

- In Germany, following a partnership of Deutsche Telekom and Google Cloud together with Ericsson, the firms announced the deployment of 5G Core cloud native network functions (CNFs) on an on-premises implementation of Google Distributed Cloud Edge (GDC Edge) [80].

- In France, Orange announced the roll out of Pikeo "Europe's first 5G standalone end-to-end network operating in a cloud-native mode" in collaboration with AWS. It will combine private 5G, IoT, cloud/edge, data and AI. It is 100% softwarised, not just the radio access network (RAN) but the core, the IT, the operational support system (OSS) and the devices[81]. The trial will soon be extended to a site in Spain. More generally, AWS is promoting a new integrated private wireless program with leading telecommunications operators.[82]

As far as messaging services are concerned, Apple and global satellite service Globalstar conducted a partnership to deliver Emergency SOS via satellite for iPhone 14 models[83]. This service allows iPhone 14 and iPhone 14 Pro models to connect directly to a satellite, enabling messaging with emergency services when outside of cellular and Wi-Fi coverage. Apple invested 450 million dollars to provide the critical infrastructure that supports Emergency SOS via satellite. This service was launched in the US and Canada in November 2022, and became available in France, Germany, Ireland, and the UK in December 2022[84].

Additionally, there are several cooperation projects regarding CAPs content and services to ISPs customers. For instance, some ECS/ECN operators, as part of their TV packages, offer promotional deals on certain large SVoD platforms. These bundles consist for example in including free subscription to a certain SVoD platform during the first months of the internet offer[85]. They are not only a way for telecommunications operators to attract new subscribers to their internet offers, but also an opportunity for the major CAPs to win over new subscribers.

[80] Deutsche Telekom, Google Cloud, Ericsson complete 5G cloud pilot, see: https://www.capacitymedia.com/article/2bbciebm867drvtxr8veo/news/deutsche-telekom-google-cloud-ericsson-complete-5g-cloud-pilot

[81] Orange announces project Pikeo, its cloud 5G network of the future, see: https://www.capacitymedia.com/article/29otdc38gbc2vnj2an5z4/news/orange-announces-project-pikeo-its-cloud-5g-network-of-the-future

[82] AWS Teams Up with Leading Telcos to Launch the 'Integrated Private Wireless on AWS' Program, see: https://aws.amazon.com/it/blogs/industries/aws-launches-integrated-private-wireless-on-aws-program AWS Teams Up with Leading Telcos to Launch the 'Integrated Private Wireless on AWS' Program, see: https://aws.amazon.com/it/blogs/industries/aws-launches-integrated-private-wireless-on-aws-program

[83] Emergency SOS via satellite on iPhone 14 and iPhone 14 Pro lineups made possible by 450 million dollars Apple investment in US infrastructure, see: https://www.apple.com/newsroom/2022/11/emergency-sos-via-satellite-made-possible-by-450m-apple-investment/

[84] Emergency SOS via satellite available today on the iPhone 14 lineup in France, Germany, Ireland, and the UK, see: https://www.apple.com/uk/newsroom/2022/12/emergency-sos-via-satellite-available-in-france-germany-ireland-and-the-uk/

[85] Disney, see: https://boutique.orange.fr/tv/disney-plus

Some examples are Orange and Disney+ in France and A1 and Netflix in Austria.[86] In general, smaller ISPs are not attractive for major SVoD providers since they do not have a sufficiently large customer base, and smaller CAPs may not be attractive for TV offers of ISPs.

Finally, in the context of business services, ISPs are also bundling their own communication services with security solutions, collaborative platforms and other services provided by large CAPs, as shown in the external study on Communication Services for Businesses in Europe commissioned by BEREC in 2022.[87]

4. Case study 1: Content delivery networks

CAPs are the main customers of a CDN provider. However, in the last few years, the largest CAPs have been investing heavily in their own CDN infrastructure and, in addition to in-house CDNs, large CAPs such as Amazon, Alibaba, Google, and Microsoft are also commercially operating CDNs to support services that are used by their cloud customers[88].

4.1. Description of the service

According to the International Telecommunication Union (ITU), a CDN is a network optimised for the distribution of digital content[89]. In addition, ITU defines a CDN as a system of distributed servers that deliver content (e.g., web pages, files, videos and audios) to users based on pre-defined criteria such as the geographic locations of users, the status of the content delivery server and the IP network connection[90]. ETSI (European Telecommunications Standards Institute) similarly describes the CDNs as follows: systems for the efficient delivery of digital objects (e.g., files with multimedia content as video on demand or other file types) and multimedia streams (e.g. live television streams) over IP networks to many end points and viewers[91]. NIS2-Directive[92] defines a CDN as a network of geographically distributed servers

[86] Disney, see https://boutique.orange.fr/tv/disney-plus and future zone, see: https://futurezone.at/produkte/a1-internet-tarife-2-jahre-netflix-gratis/402636806

[87] BoR (22) 184, External Study on Communication Services for Businesses in Europe: Status Quo and Future Trends, 12.12.2022, see: https://www.berec.europa.eu/en/document-categories/berec/others/external-study-on-communication-services-for-businesses-in-europe-status-quo-and-future-trends

[88] WIK. Competitive conditions on transit and peering markets Implications for European digital sovereignty, 2022, see: https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/Digitisation/Peering/download.pdf?__blob=publicationFile&v=1

[89] ITU-T F.750 Metadata framework, see: https://www.itu.int/rec/T-REC-F.750-200502-I/en

[90] ITU-T Y.2084 Distributed service networking content distribution functions, see: https://www.itu.int/rec/T-REC-Y.2084-201506-I/en

[91] ETSI TS 182 032 V1.1.1 (2013-04), CDN Interconnection Architecture, see: https://www.etsi.org/deliver/etsi_ts/182000_182099/182032/01.01.01_60/ts_182032v010101p.pdf
ETSI TS 102 990 V1.1.1 (2012-11), Media Content Distribution (MCD); CDN Interconnection, use cases and requirements, see: https://www.etsi.org/deliver/etsi_ts/102900_102999/102990/01.01.01_60/ts_102990v010101p.pdf

[92] Article 6 (32) of the Directive EU 2022/2555 (NIS2).

for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers.

CDNs entail a change in the way data/content is distributed over the internet. While this was originally based on a centralised scheme, the emergence of CDNs led to a distributed system to facilitate access to the content. This distributed system optimises the transport of traffic and provides end-users with an improved experience when consuming content.

A CDN provider is the entity that is responsible for providing the infrastructure necessary to distribute content from content providers (e.g. audiovisual content providers, media companies, internet advertising companies, etc.) to end-users in real time[93]. This infrastructure may comprise the servers, the connectivity between servers and the connectivity with ISPs. To achieve this connectivity, CDN providers have a wide range of possibilities from establishing and controlling end-to-end connectivity between their servers (with their own means of transmission), using third-party connectivity (such as leased lines) or sending their traffic over the internet (best effort). CDN providers also interconnect their infrastructure at peering interconnection points with ISPs, with other CDN providers to extend their footprint, or locate their edge servers within the ISPs' networks. This duality, in which some CDN providers act as applications on top of the internet, while others have their own infrastructure and therefore do not need to acquire connectivity from an ISP, was highlighted in the BEREC Report "An assessment of IP interconnection in the context of Net Neutrality"[94].

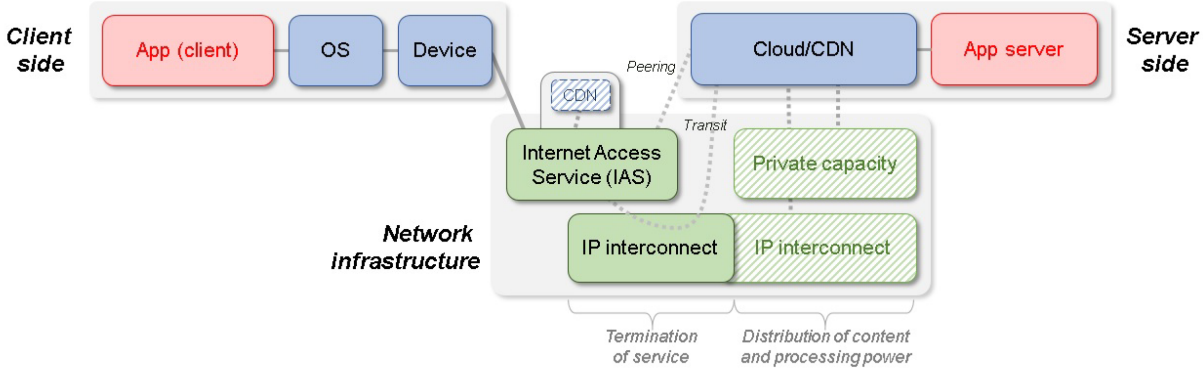
The main functions of a CDN provider are the distribution and replication of content across different servers in the network from the origin server where the content provider has uploaded its content and the routing of end-user requests to the nearest servers where content is hosted and cached. This makes the transmission of content over the internet more efficient and decreases latency.

In particular, the strategy used to define which CDN node serves each user is a crucial point of CDNs' functioning and potentially affects the traffic generated on ISPs' networks because it can change the routes and links to be used to distribute traffic. Typical strategies by CDN providers involve identifying the most efficient node based on parameters such as geographic distance, traffic load on the node, network conditions (e.g. congestion) and network distance (e.g. using IP anycast).

[93] ITU term "*Content delivery network (CDN) provider*": "*The special organization or company in charge of providing the infrastructure needed to deliver the content service provider's (CSP) contents to the end users in real time mode*", see: https://www.itu.int/net/ITU-R/asp/terminology-definition.asp?lang=en&rlink=%7b4E8D5A84-A95F-4195-BFF7-01D4D5DA7CE8%7d

[94] BoR (12) 130, An assessment of IP interconnection in the context of Net Neutrality, 06.12.2012, see: https://www.berec.europa.eu/en/document-categories/berec/reports/an-assessment-of-ip-interconnection-in-the-context-of-net-neutrality (p. 15)

Figure 5. Generic overview of the functioning of CDN



<u>Legend</u>*: *Green *boxes represent the connectivity segments/services;* ***Blue*** *boxes represent the hardware and software from the device or cloud server;* ***Red*** *boxes represent the client-server application that is being used.*

Source: BEREC

The Figure 5 above shows a simplified diagram of the connections between the CDN provider, its servers, the IAS and the end-user accessing the content (through their device). On the one hand, the distribution of content between the different servers of the CDN provider (i.e. servers in the diagram are in the blue box called Cloud/CDN) uses its own infrastructure (private capacity) or IP interconnections with third parties (i.e. striped green boxes). CDNs can also reach agreements to deploy their servers within the IAS network (i.e. blue striped box). In order for users to access content hosted on the servers closest to their location, CDN providers must be connected to the IAS. The diagram shows that these connections can be made by transit (public or private), direct peering or by hosting the servers within the IAS network. In this way, the end-users through their access to the IAS can access the content distributed and hosted by the CDN provider.

4.2. Business models

A decade ago, the major CAPs relied heavily on commercial CDNs[95] (e.g. Akamai, Cloudflare, etc.) for their services. However, there has been a significant shift since then: large CAPs have developed their own CDNs, tailored to meet their specific traffic requirements, and now provide these services in-house ("insourcing"), or, in some cases, also to third parties (primarily in the field of cloud services). As a result, the creation of value has moved from commercial CDNs towards the large CAPs with their own CDNs. It should be noted that several

[95] For commercial CDNs, we refer to public CDN (to third parties) as they are described below in this section.

telecommunication operators have built their own CDNs to offer audio-visual content services to their end-users and others have extended their services to third parties with CDN services[96].

The share of traffic handled via CDN varies greatly among large CAPs: for instance, Netflix delivers (almost) 100% of its traffic via its own CDN[97], while Google 50%[98]. Moreover, some CAPs may use only one CDN while others rely on several CDNs (multi-CDN approach) thereby increasing resiliency and mitigating risks.

The diversity of CDN providers, as well as their location and interconnection modalities, varies according to the content distribution requirements and costs (or their own content distribution requirements in case of a private CDN)[99]. Some CAPs do not need or cannot afford to upgrade their content distribution and therefore rely on basic internet functionality to distribute their content. In contrast, other CAPs, due to their volume or very particular needs, build their own CDNs, thus reducing distribution costs and optimising the performance of their networks.

There is a wide range of CDN providers that offer services to third parties. These providers can be regional or global, niche or generalist, and there is a wide variety of business models in the market.

Depending on the business model implemented for the specific online content to deliver (e.g. live video, video on demand, games, text, etc.), several approaches can be considered based on providers' perspective:

- Private CDN (self-provisioning): in this case a CAP owns and operates its own CDN infrastructure (e.g. Netflix, Dazn, Meta, Apple) to fulfil its own content distribution needs. This solution typically provides better security and more control over data and performance, but is characterised by higher upfront costs.

- Public CDN (open to third parties): in this case the CAP relies on a CDN provider (e.g. Akamai or Cloudflare) which manages the infrastructure and distributes the CAPs' content. Compared to the private CDN, for a CAP this solution offers better flexibility

[96] See: https://globalcarrier.telekom.com/business-areas/internet-content/cdn-solution; see: https://www.cdnplanet.com/cdns/lumen/; https://www.business.att.com/products/cdn.html, see: https://globalcarrier.telekom.com/business-areas/internet-content/cdn-solution; etc.

[97] This is the consequence of investing by Netflix in Open Connect Appliances (OCAs) which are a combination of local servers. Since the launch of Open Connect in 2011, Netflix has spent over 1billion euros to develop and deploy 14.000 OCAs across 142 countries. Netflix, A cooperative approach to content delivery, 2021, see: https://openconnect.netflix.com/Open-Connect-Briefing-Paper.pdf (p. 20)

[98] WIK. Competitive conditions on transit and peering markets Implications for European digital sovereignty, 2022, see: https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/Digitisation/Peering/download.pdf?__blob=publicationFile&v=1 (p.28)

[99] Stocker, Volker; Smaragdakis, Georgios; Lehr, William; Bauer, Steven. Conference paper: Content may be King, but (Peering) Location matters: A Progress Report on the Evolution of Content Delivery in the Internet. 27th European Regional Conference of the International Telecommunications Society (ITS), Cambridge, United Kingdom, 7th - 9th September 2016, see: https://www.econstor.eu/handle/10419/148708

with fewer initial costs and can be more cost-efficient in specific cases (e.g. small CAPs).

- Mixed-use CDN: in this case, the CDN infrastructure deployed by the CAP has a double purpose - the CAP manages its own infrastructure to distribute its content, and with the remaining unused capacity provides CDN services to third parties. Thus, the CDN has the characteristics of the two previous approaches. This is the case of e.g. Google Cloud, Amazon Cloudfront or Microsoft Azure.

In all the above cases, CDNs can be built based on a unique infrastructure or on multiple infrastructures, owned and/or provided by third parties, following a multi-CDN approach. This latter strategy allows CAPs to improve their footprint, as well as the resilience and the scalability of their services.

4.3. Overview of the market

According to Cisco, in Europe, depending on the countries, the volume of internet traffic passing through a CDN was up to the 88% of total internet traffic and up to the 98% of total video traffic in 2022.[100]

Overall, the global CDN market around the world is expected to grow from 14 billion euros[101] in 2021 to 36 billion euros in 2026 at a CAGR of 18.4%, since 2012[102]. The European CDN market stood at around 3,2 billion euros in 2019 and is projected to grow at a CAGR of over 29% to reach 16 billion euros in 2025[103]. The growth of this market is attributed to the increase of both internet penetration and consumption of audio-visual content, and to the adoption of CDN by various enterprises, including SMEs. In addition, in the coming years, this market is expected to continue to grow due to the following trends: the rising of cloud-enabled services

[100] VNI Complete Forecast Highlights, Western Europe, see: https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Western_Europe_Consumer_Highlights.pdf
VNI Complete Forecast Highlights, Rest of Western Europe (part of Nordics), see: https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Rest_of_Western_Europe_2022_Forecast_Highlights.pdf
VNI Complete Forecast Highlights, Central and Eastern Europe, see: https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Central_and_Eastern_Europe_2021_Forecast_Highlights.pdf
VNI Complete Forecast Highlights, Rest of central and eastern europe, see: https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Rest_of_Central_and_Eastern_Europe_2022_Forecast_Highlights.pdf

[101] Certain values sourced in dollars have been converted to euros for consistency in the document. For the conversion, OECD exchange rates have been used, see: https://data.oecd.org/conversion/exchange-rates.htm#indicator-chart

[102] ReportLinker, Global CDN Industry: Strategic Insights and Predictions, 2023, see: https://www.reportlinker.com/p06311708/Content-Delivery-Network-Global-Market-Report.html

[103] ReportLinker, Europe Content Delivery Network Market - Competition Forecast & Opportunities, 2025, see: https://www.reportlinker.com/p05615125/Europe-Content-Delivery-Network-Market-Competition-Forecast-Opportunities.html?utm_source=PRN

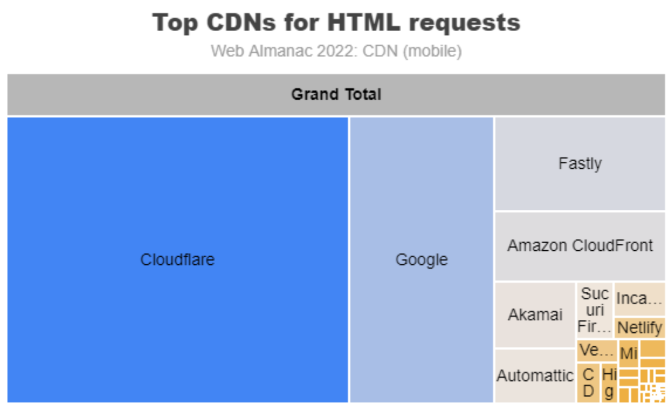
that allow for website security, increase of content availability, lower network latency, Internet of Things (IoT), 5G Infrastructure, use of real-time analytics enabled by AI across the globe.

The CDN market may be segmented based on several criteria: type of content (video, media & communication, retail & e-commerce, static and dynamic), type of client, service provider (cloud service providers, telecommunication operators, content delivery network & others), solution (media delivery, web performance optimization, cloud security, etc.) and country/region.

It is not straightforward to obtain CDNs' market shares as they vary between sources and according to whether they are measured on a traffic, customers or revenue basis. However, it can be concluded from the information gathered that this market is concentrated:

a) based on traffic, the top CDN providers globally for web browsing (based on HTML requests) on mobile[104] in 2022 were Cloudflare, Google, Fastly, Amazon CloudFront, Akamai and Automattic, with a market share of 92% (see Figure 6).

Figure 6. Top CDNs for HTML requests on mobile



***Legend**: Box plot showing the top CDN providers serving HTML requests. Cloudflare tops the list by serving 52% of the HTML requests followed by Google at 22%, Fastly at 9%, CloudFront at 6% and Akamai and Automattic at 3%.*

Source: Web Almanac[105]

b) based on customers or websites, according to ENISA, CDN providers can be ranked according to the number of websites served from the "top 10 million" list. With this

[104] Web Almanac, CDN, see: https://almanac.httparchive.org/en/2022/cdn
[105] Web Almanac, CDN, see: https://almanac.httparchive.org/en/2022/cdn

approach, Cloudflare would have over 80% of the market share. However, the International Data Corporation (IDC) also identifies a concentrated market around few CDN providers: Akamai is leading this list, followed by Amazon, Cloudflare and Alibaba[106].

c) Based on several measures, including revenues, Akamai, Amazon CloudFront, and Cloudflare are the leaders of the market[107]. The CDN market has a large number of smaller providers, but the top three CDN providers controlled in 2020 more than half the market. With just over 2.1 million customers[108], the vast majority of CDN customers spend less than 11,400 euros annually on CDN services. A small portion of CDN customers (just less than one percent) spend more than 95,000 euros, but contribute to an estimated 10% of the total revenue for the top 10 CDN providers.

Other sources[109] point out that the major players in Europe are Akamai, Amazon, CenturyLink, AT&T, Verizon, Google, Limelight Network, Internap Corporation, Tata Communications and Microsoft, that together account for more than 50% of the market share.

From the previous sources, it can be concluded that although there are many public CDN providers in the market, the market is concentrated around few providers. Although depending on the ranking criteria the largest leader may change, the top six, which have a combined market share above 50%, are generally the same: Akamai, Amazon, Cloudflare, Alibaba, Google and Microsoft. This concentration may be due to the investments required in infrastructure to ensure a large footprint and to ensure good coordination of locations as close to the user as possible.

4.4. Relations among the main stakeholders involved

Figure 7 shows the relations between content providers (i.e. content provided by a Business, or content generate by end-users), CDN providers, IAS and content users (client).

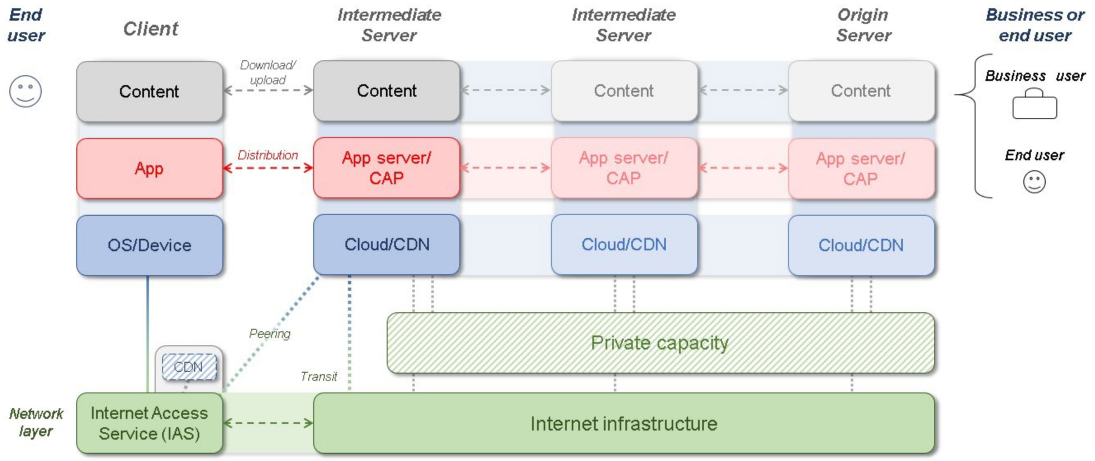
[106] See ENISA, “Short paper on the security and operation of content delivery networks”, 2022 – available under request.

[107] 2020 CDN Market Report, Intricately, see:https://go.hginsights.com/rs/214-HYO-692/images/2020IntricatelyCDNMarketReport.pdf

[108] By customers, we mean small and medium-sized CAPs that turn to CDN providers to have their content accessible in a good footprint.

[109] ReportLinker, Europe Content Delivery Network Market - Competition Forecast & Opportunities, 2025, see: https://www.reportlinker.com/p05615125/Europe-Content-Delivery-Network-Market-Competition-Forecast-Opportunities.html?utm_source=PRN

Figure 7. Main relations between content providers, CDN providers, ISP and end-users



***<u>Legend</u>*: *Green* boxes represent the connectivity segments/services; *Blue* boxes represent the hardware and software from the device or cloud server; *Red* boxes represent the client-server application that is being used.*

Source: BEREC

From the content providers' point of view (business or end-user side in the right of Figure 7), their content is distributed in the geographic area of their interest, and they value the quality of customer experience (end user/client side in the left of Figure 7) when accessing their content, which is why they use CDN providers. For their part, CDN providers charge content providers for several features, such as their footprint, the transmission capacity of their content, whether or not they have a private backbone (dedicated connectivity as opposed to using the basic functionality of the internet to send content, see green and striped green boxes below Cloud/CDN boxes) etc. End-users (customers of the content provider) are usually not aware of the existence of a CDN (they know their ISP and their CAP) and value their experience of accessing content on parameters such as fast loading of content, low latency or high definition in the case of video content. In addition, the end-user pays the access provider for his internet connection. The ISP, for its part, may be interconnected with the CDN provider through a peering agreement whose capacity (and costs) must be increased to ensure that the link does not become saturated. Some ISPs host CDN servers on their own network (on-net CDN see blue striped box next to IAS box) in order to reduce capacity costs (e.g. peering interconnection, backbone and backhaul links) for the content consumed by their end-users and locate content as close to the end-users as possible (see CDN box above IAS box in Figure 7).

The arrangements between CDN providers and ISPs may vary depending on the scenario or market observed.[110] CDNs initially generated wholesale revenues for Tier 1 ISPs, large

[110] The relation between CDN providers and ISPs will also be addressed in the BEREC report on the IP interconnection ecosystem.

ISPs[111] received from smaller ISPs that paid IP transit fees. As CDNs moved closer to the consumer, smaller ISPs started to host CDNs, resulting in lower wholesale revenues for the Tier 1 ISPs[112]. Traffic coming from on-net CDNs is growing significantly (for example, on-net CDN traffic in France nearly doubled between 2019 and 2020), as a CDN hosted in an ISP's access network lowers the cost supported by CAPs and the ISPs for IP transit[113] because there is no need to transmit that content via the Tier 1 ISP, this fact was pointed out in BEREC Report on the topic[114]. In this scenario, the on-net distribution of content by CDNs reduces the potential revenues of the Tier1 ISPs for their wholesale transit services so that one activity impacts on the revenues of the other. In the case of mixed use and public CDN providers, CAPs could be seen as competitors of Tier 1 ISPs.

However, there are other scenarios where content providers with their CDN and ISPs can create a mutually beneficial relation. For instance, in Italy, the transmission of Italian football championship via the live streaming service Dazn constitutes an example of the dynamics between CAPs and ISPs, and the crucial role played by NRAs in this context. In March 2021, the streaming service Dazn was awarded football championship broadcasting rights for 2021-2024. In the same period, Dazn and TIM, Italy's main operator, signed an agreement that entailed, *inter alia*, TIM to provide technological support to Dazn. Since football is the most followed sport in Italy, the transition of the transmission of championship matches from traditional satellite and terrestrial Pay-TV services to an OTT live streaming service constituted an unprecedented break away from traditional broadcasting and a further impetus to the development of very high-capacity networks (VHCN). This transition involved potential competition and technical issues on fixed and mobile markets. In this context, AGCOM adopted the Decision 206/21/CONS[115] in order to promote competition among operators and prevent potential network congestion issues: with this Decision, Dazn was asked, inter alia, to provide and install caches of its own CDN (Dazn Edge) in the network of the main alternative operators, in order to prevent congestion issues, guaranteeing a better QoS and the technical and economical sustainability of live streaming traffic growth. Moreover, the Decision states

[111] Large ISPs that do not pay for IP transit.

[112] Pages 10 and 20 Steve Esselaar, Christoph Stork, November 2022, Competition and investment in the Internet value chain in Europe, see: https://www.researchgate.net/publication/365762548_COMPETITION_AND_INVESTMENT_IN_THE_INTERNET_VALUE_CHAIN_IN_EUROPE

[113] "On-net CDN traffic comes at the expense of peering and transit traffic". Competitive conditions on transit and peering markets. WIK-Consult report, see: https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/Digitisation/Peering/download.pdf?__blob=publicationFile&v=1

[114] BoR (12) 130, An assessment of IP interconnection in the context of Net Neutrality, 06.12.2012, see: https://www.berec.europa.eu/en/document-categories/berec/reports/an-assessment-of-ip-interconnection-in-the-context-of-net-neutrality (Conclusion (g))

[115] See: https://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_FnOw5lVOIXoE&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_count=1&_101_INSTANCE_FnOw5lVOIXoE_struts_action=%2Fasset_publisher%2Fview_content&_101_INSTANCE_FnOw5lVOIXoE_assetEntryId=23770627&_101_INSTANCE_FnOw5lVOIXoE_type=document.

that the number of CDN caches (and so the related bandwidth) has to be proportional to the operators' market share.

Finally, IXPs also play a crucial role in the delivery of CDN content to ISPs' networks, especially in the case of smaller ISPs not deploying on-net caches (the number of IXPs has almost doubled in the last 10 years)[116]. Therefore, the mentioned growth of CDN traffic implies the need for the ISPs to upgrade their link capacity at the IXPs' premises where CDN providers are interconnected.

5. Case study 2: Submarine cables

5.1. Description of the service

The first submarine cable was installed in the 19th century, and its technology has been evolving ever since. Currently, submarine fibre optic cable networks[117], which are part of the global international ECN infrastructure, are crucial to the global economy and play a key role in maintaining a robust global network infrastructure that supports the seamless functioning of the internet and ECSs. In 2023, more than 529 submarine cable systems, and 1444 cable landings stations (CLS)[118] were responsible for carrying 99% of all international ECS traffic[119], including the services provided by CAPs to consumers.

The legal and regulatory regimes applicable to these infrastructures differ among the countries and the regions that the international submarine cables connect. These legal and regulatory provisions span from deployment to environment protection and infrastructure security. BEREC has published a report on the general authorisation and related frameworks for international submarine connectivity that aims to clarify the general authorisation and related frameworks applicable to international submarine connectivity[120] .

5.2. Business models

In recent years, the international submarine cable connectivity market has witnessed significant changes, particularly with the involvement of large CAPs like Google, Meta,

[116] Competitive conditions on transit and peering markets. WIK-Consult report: https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/Digitisation/Peering/download.pdf?__blob=publicationFile&v=1

[117] The ITU sets out a comprehensive recommendation on the definition of terms relevant to optical fibre submarine cable systems, see https://www.itu.int/rec/T-REC-G.972-202010-I/en

[118] Currently active or under construction.

[119]EC https://emodnet.ec.europa.eu/en/map-week-%E2%80%93-submarine-telecommunication-cables

[120] BoR (23) 214, Draft BEREC Report on the general authorisation and related frameworks for international submarine connectivity, 07.12.2023, see: https://www.berec.europa.eu/en/document-categories/berec/reports/draft-berec-report-on-the-general-authorization-and-related-frameworks-for-international-submarine-connectivity

Microsoft and Amazon investing in these infrastructures. On the demand side, there has been an extraordinary surge in global internet traffic, demanding substantial increases in capacity for international transit. Simultaneously, on the supply side, the ownership structure of international submarine cables is undergoing a profound transformation, reshaping the traditional business model.

One crucial development is the shift of large CAPs from being mere direct or indirect customers of wholesale capacity to becoming investors and owners of transport network infrastructure, particularly submarine cables. This transition began with Google's investment in the Unity cable consortium in 2010, followed by Meta, Microsoft and, most recently, Amazon, who have either directly invested in or been major pre-sale purchasers of new submarine cable systems.

In the past, traditional operators and telecommunication carriers developed business cases aimed at deploying submarine routes capacity to carry traffic for their customers. Their primary objective was to have transnational transit capacity for their own retail services and for directly selling capacity to third parties (leased lines/circuits), with a substantial portion of their revenue stemming from leased circuits, including directly or indirectly from large CAPs. However, with large CAPs increasingly building their own transport networks (including submarine cables), a relevant part of the traffic originating these revenues is being internalised by CAPs, which significantly impacts the business model of carriers/traditional ISPs who have to reorganise their position in the market.

The primary focus of large CAPs' investment is to interconnect their data centres and regional PoPs to data centres. This strategy aims to strengthen their self-reliance and operational efficiency (including higher QoS by e.g. reducing latency) by connecting data centres close to the CLSs[121]. In the routes where they invest in their own infrastructure, such large CAPs are no longer reliant on transit (e.g. Tier 1) network operators to provide capacity.

The financing and ownership models for submarine cables fall into three categories: multi-investors (consortium), single investors, and Public Private Partnerships (PPP). When submarine cables are developed by a consortium of investors, they typically are based on co-ownership and co-operation, i.e. fibres are owned individually by members of the consortium, while the ownership and costs of common infrastructure is shared. Individual ownership of fibres means each consortium member can operate them as separate and independent networks. Each member is responsible for its own transmission equipment and all physical and logical connections to its own fibres[122]. Multi-investor models have historically been the

[121] In particular, large CAPs have preference for landing locations that provide cost saving benefits to reduce operational expenditure, such as locations that provide sufficient availability and efficient use of energy for data centres and direct backhaul terrestrial interconnection. In specific, large CAPs tend to prefer places with availability of elements that allow for an efficient cooling system, such as the north of Europe or the existence of alternative energy. These locations also allow for terminating the submarine line terminal equipment in a carry neutral data centre.

[122] Information provided by Stakeholders to BEREC Digital Markets Questionnaire that was sent to large CAPs in July 2023.

most common, but single investor models have gained popularity, especially with large CAPs entering the market with their own cables, due to their significant financial resources.

Initially, large CAPs relied on carriers/traditional ECN/ECS operators, but now they are expanding their partnerships and started working with dark fibre providers, and mobile networks operators.

Large CAPs predominantly use the capacity on the submarine cables for their own internal needs, particularly for interconnecting their data centres. Consequently, these cables serve a component of their own supply chain for delivering data services. However, if there is capacity remaining, some swap it with other owners of submarine cables. For instance, Microsoft submarine cables are part of the supply chain for Azure cloud applications and the rest of the capacity is exchanged with other actors operating submarine cables in similar routes. Notwithstanding, from BEREC’s questionnaire, one CAP has notified to have swapped fibres with owners of other submarine cables, while another has swapped some fibre pairs with providers on other systems or is in the process of negotiating fibre swaps with other actors also owning their own submarine cables.

The ownership structure has evolved considerably, with large CAPs emerging as the largest deployers of the newly submarine cable systems in recent years. Google stands out as the sole owner of eight[123] submarine cables, while Meta, Microsoft, and Amazon have often joined consortia that include specialised ECS providers with expertise in operation and deployment of submarine cables.

In cables deployed by consortia, capacity is divided into Minimum Investment Units (MIUs) and sold in terms of Indefeasible Rights of Use (IRU) through Capacity Purchase Agreements (CPAs). Capacity on private cables may be also sold but mostly on different terms. IRU is the effective long-term lease of a portion of the capacity of an international cable and specified in terms of a certain number of channels of a given bandwidth. The CPAs often forbid resale of the capacity ownership and usually grant ownership for 25 years (the expected lifespan of submarine cables). The service gives a large-scale ISP the ability to assure its own customers of international service on a long-term basis.[124]

The business models developed in consortia are also changing. More recently, there has been a push towards the co-construction/co-ownership model under leadership of one of the members of the consortium. Another model introduced by large CAPs is the open access model, which allows investors to have their own fibre pairs and those fibre pairs can be part

[123] Dunant, Equiano, Grace Hopper, and now Nuvem with landing points in Europe, and Curie, Firmina, Junior, Topaz with landing points outside Europe even if is co-owner of more than 10 other submarine cables with landing stations outside Europe.

[124] European Commission, Study to Monitor Connectivity, Connecting the EU to its partners though submarine cables: final study report, 2020, see: https://op.europa.eu/en/publication-detail/-/publication/a0b01654-9394-11ec-b4e4-01aa75ed71a1

of their network and they can be effectively operated independently from the rest of the owners or the actual cable owner itself.

Strategically, large CAPs are investing in submarine cables because it provides them with increased control over assets. The demand they experience, globally, growing at unprecedented pace means that their need for additional bandwidth outpaces their ability to purchase it in a timely manner. Although they are deploying their own infrastructure, large CAPs are still buyers of international capacity from carriers/transit third parties because their own infrastructure, in some cases, is still not sufficient to serve all demand, or simply because they have not (yet) deployed any submarine cables in the corresponding route.

5.3. Overview of the market

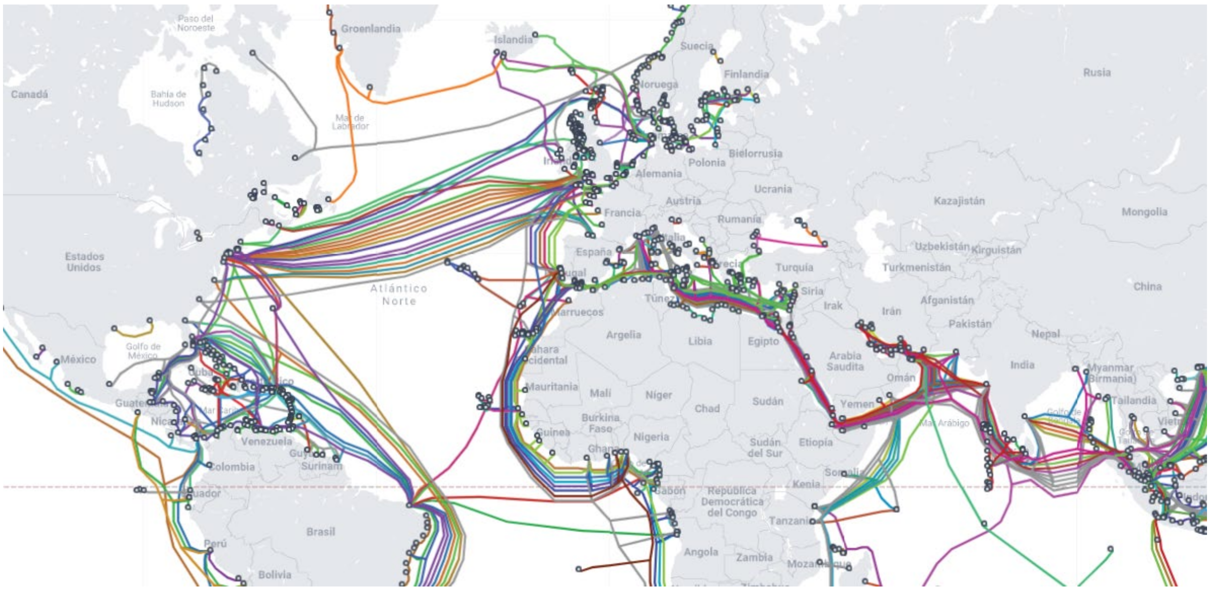
The EU is connected with about 250 active cables that ensure connectivity to the global internet. Denmark, France, Italy, Portugal, Spain, and the islands of Malta and Ireland are the EU Member States with greater submarine cable connectivity.[125] According to TeleGeography, demand for international bandwidth is nearly doubling every two years. Between 2019 and 2021, international bandwidth used by global network operators doubled to reach 3,900 Tbps.[126]

In 2003, the total capacity across the Atlantic was less than 100 Terabit/s while now, thanks to the innovation on increased number of fibres per cable (e.g. 24 fibres), multicore fibres, and more efficient modulations and multiplexing, the most recently deployed submarine cables have capacities in the order of 500 Terabit/s.

[125] German Council on Foreign Relations, Protecting the EU’s Submarine Cable Infrastructure, 10.07.2023, see: https://dgap.org/en/research/publications/protecting-eus-submarine-cable-infrastructure

[126] TeleGeography, The State of the Network, 2023, see: https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/state-of-the-network-2023.pdf?utm_campaign=Prospect%3A%20Networks%202&utm_medium=email&_hsmi=60033117&_hsenc=p2ANqtz-852mvV2MAgBFvjeEsmQexXYDCwdEwtIC5p3K8TMgiPug57BZ7cxeiACBr5bMn7qAa1Fs9MAXVFVZim31gRoOiTSOg9sg&utm_content=60033117&utm_source=hs_automation

Figure 8. Subsea Cables Map in Europe, 2023



Source: Telegeography[127]

In the past, the need for increased international capacity was largely met by carrier networks. However, nowadays, large CAPs like Amazon, Google, Meta and Microsoft are building their own infrastructure for their services. These companies accounted for 69% of all international capacity usage in 2021. Large CAPs have added capacity, across every region, at a compound annual rate of at least 51% between 2017 and 2021, compared to a rate no higher than 45% for all the others. [128]

By 2017, traffic generated by large CAPs had surpassed other sources of traffic using international capacity. In the period of 2016 to 2020 large CAPs were already the driving force behind 36% of systems that went into service[129]. For the period spanning 2019 to 2023, these large CAPs have been behind 24 systems in all the world, accounting for 23.5% of the 102 total systems that went into service, and in 2023 alone, large CAPs accounted for a substantial portion of all new system builds. For the upcoming period of 2024 to 2028, 14% of the 56 planned systems in the world are expected to be driven by large CAPs.[130]

The capacity requirement for large CAPs varies extensively by route. Large CAPs started around 10 years ago to invest in subsea cables to have more control over the quality (security, create extensive connectivity, diversity for a reliable network and sufficient capacity for current and future applications). Large CAPs, therefore, use an investment strategy that prioritizes the

[127] Submarine Cable Map, see: https://www.submarinecablemap.com/

[128] Submarine Cable Map, see: https://www.submarinecablemap.com/

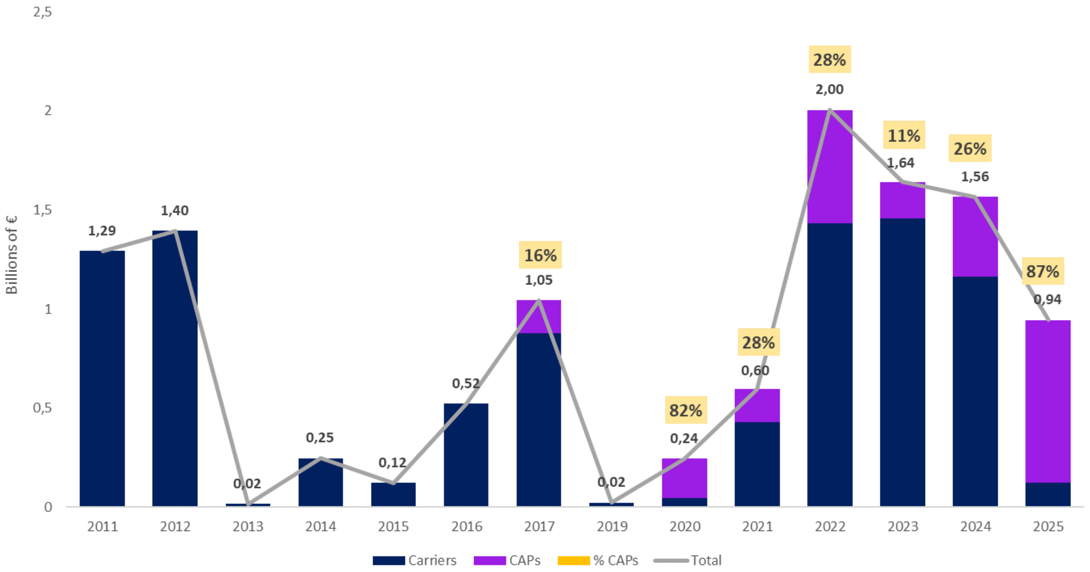
[129] European Commission, Study to Monitor Connectivity Connecting the EU to its partners though submarine cables. Final Study Report, 2020, see: https://op.europa.eu/en/publication-detail/-/publication/a0b01654-9394-11ec-b4e4-01aa75ed71a1

[130] Submarine telecoms forum Industry report 2023-2024, see: https://subtelforum.com/industry-report/

need to interlink their data centres and major interconnection points. As such, they often take significant capacity on trans-continental routes typically connecting their data centres and interconnection points, while focusing much less than traditional carriers on other routes. Additionally, while most telecom carriers rely on landing stations where many submarine cables connect, large CAPs can directly connect their own data centres without having to connect to existing landing stations.

Since 2017 large CAPs have invested over 2,4 billion euros in new cables entering or already in service with landing points in Europe. This investment represents 10 subsea cables with a total length of 74,141 km, with at least 1,684 Tbps of design capacity and 125 fibre pairs.[131]

Figure 9. Investment in submarine cables done/planned in Europe based on the date for ready for service



Source: BEREC, based on data from Subsea Cable Almanac and Telegeography

Most of these investments are done via consortium and large CAPs typically own only one or two pairs of fibre cables.

[131] BEREC, based on Subsea Cable Almanac and Telegeography.

Table 1. Overview of Large CAPs' investment in Subsea Cables in Europe, since 2015

Name	Planned or In-service	CAP	Ownership	Year	Cost (M€)	Countries in Europe
EXA Express	In-service	Microsoft	Major capacity buyer	2015	114	Ireland, United Kingdom
AEC-1	In-service	Meta, Microsoft	Major capacity buyer	2016	285	Ireland
MAREA	In-service	Amazon, Meta, Microsoft	Major capacity buyer, Part Owner, Part Owner	2017	156,8	Spain
Havfrue/AEC-2	In-service	Amazon, Meta, Google	Major capacity buyer, Part Owner, Part Owner	2020	190	Denmark, Norway, Ireland
Dunant	In-service	Google	Sole Owner	2021	156,8	France
Equiano	Planned	Google	Sole Owner	2022	356,3	Portugal
Grace Hopper	Planned	Google	Sole Owner	2022	161,5	Spain, United Kingdom
Havhingsten/CeltixConnect-2	In-service	Meta	Part owner	2022	22,3	Ireland, United Kingdom
Havhingsten/North Sea Connect	In-service	Meta	Part owner	2022	1.5	Denmark, United Kingdom
2Africa	Planned	Meta	Part owner	2023	878,7	Spain, France, Italy Portugal, United Kingdom, Greece
Amitie	Planned	Meta, Microsoft	Part owner	2023	173,2	France, United Kingdom
Blue	Planned	Google	Part owner	2024	380	France, Italy, Greece, Cyprus
SEA-ME-WE 6	Planned	Microsoft	Part owner	2025	475	France
Anjana	Planned	Meta	Sole owner	2024	N/A	Spain
Nuvem	Planned	Google	Sole owner	2026	N/A	Portugal
Beaufort	Planned	Amazon	Part owner	2024	N/A	Ireland, United Kingdom

Source: BEREC, based on data from Subsea Cable Almanac[132], Submarine Cable Networks and Telegeography (Cost represents total costs for the whole systems, not per investors)

[132] Submarine Cable Almanac, see: https://subtelforum.com/almanac/

5.4. Relations among the main stakeholders involved

In the context of submarine cables, the main actors are ECN/ECS providers, large CAPs and companies specialised in deploying and maintaining these submarine cables.

This shift in ownership has also led to changes in stakeholders' relations within the industry. Traditionally, telecommunication operators played a central role in deploying submarine cables, setting up consortia among operators from different countries to invest in and share cable capacity. In the past, telecommunication operators were the ones deploying this type of infrastructure for their own use, including assets to lay the submarine cable as specialised vessels for this purpose. Less than a decade ago, large CAPs were not involved in the deployment of submarine cables and were mere users of the infrastructure via the connection services they contracted with telecommunication operators in different countries. Although this model of setting up consortia to deploy new cables still applies, the increasing traffic managed by large CAPs and the deployment of their own data centres and CDNs have led large CAPs to generate sufficient scale in order to make deploying their own submarine cable become a viable business strategy, marking a significant departure from their past role as mere buyers of telecommunication operator services.

Simultaneous investments on new cable systems also directly influences the future availability of manufacturers and those involved in the construction and maintenance of such systems to respond to market demands. As resources are scarce, the pressure from large CAPs to build new submarine systems and maintain existing ones, directly influences the responsiveness of suppliers and maintenance providers. There exist only approximately 50 cable ships in the world, which are under very strong pressure to meet market demand.

The impact of large CAPs on access to capacity is significant. Traditional telecom service providers may see reduced roles in transcontinental connectivity, while large CAPs deploy cables primarily in established routes. Still, as large CAPs deploy submarine cables primary for their own use, traditional telecommunication providers play a key role on the transmission of data for other CAPs, connecting areas which are not economically interesting for large CAPs, as well as centres of education, research and innovation in different continents. The future dynamics may also depend on regulatory factors and the potential entry of new players.[133]

The international submarine cable industry is undergoing substantial transformation due to the increasing involvement of large CAPs as infrastructure owners. This shift has profound implications for connectivity, competition, and infrastructure investment within the sector.

[133] For a more detailed analysis of the stakeholders involved in the value chain for deployment and use of submarine cables, see section 5.4 above

5.5. Issues at stake

Submarine cables are strategic assets not only for traditional operators and large CAPs, but also for administrations, both because most internet traffic traverse international submarine cables and because islands (being insular countries or countries comprising archipelagos or islands) are connected to the rest of the world via submarine cables.

First of all, there is a question on resilience, as an outage in a submarine cable being the only high-capacity infrastructure connecting the territory implies that key critical electronic communication services will not work. Although submarine cables are a very robust infrastructure, along its life cycles (estimated in around 25 years), breakage and malfunction may happen, partially due to human marine activity (e.g. fishing, anchoring) or natural causes (e.g. volcanic eruptions). Availability of several submarine cables connecting the territory allows for additional resilience. Europe is well connected via submarine cables and most intercontinental routes are well protected in this sense, having several different cables deployed by different actors connecting EU coastal countries especially to North America.

The investment by large CAPs is mainly focused on deploying submarine cables connecting different European countries with North America. As shown in Figure 8, the transatlantic connection with the USA and Canada is already served by a multitude of submarine cables. As a consequence, investments by large CAPs in these routes which are already very resilient only increase resilience for EU submarine connections to a small extent.

In this line, there appears to be a shortage of submarine cables between the EU and Latin America, since there are only two submarine cables connecting Europe with Brazil and Argentina: Ellalink (a cable recently deployed by Islalink) and ATLANTIS-2 (deployed in 2000 by a consortium of traditional telco operators and nearing the end of its estimated life). Large CAPs have not and, to the knowledge of BEREC, do not have plans to deploy submarine cables to connect Europe and Latin America, implying that a very relevant part of the traffic between Europe and Latin America is not affected by CAP deployments and will continue to be transmitted via the USA, adding costs and increasing risks associated with data sovereignty for both the EU and Latin America.

As presented in previous sections, CAPs are deploying submarine cables in order to connect their data centres and in routes already well-served by other cables. It is therefore unlikely that more secondary routes (being national or international) will be covered by large CAPs. In this context, it is important to ensure that submarine cables in these more secondary routes will be renewed in due time (part of them are nearing their economic life[134]), and in some situations where the business model for private investment does not hold, public funding might be needed to respond to this specific but important needs in terms for connectivity for Europe.

[134] The economic life of submarine cables is around 25 years, and it depends on many different factors. At a certain moment, the cost of maintenance and repairing faults in the long term is higher than the investment for a new submarine cable.

One area of concern for operators deploying submarine cables is the potential shortage of vessels which deploy and maintain these cables. There are only around 50 of these cable ships around the world, most of them more than 20 years old, and there is a strong demand pressure both for deployment and repairment of submarine cables, leading to high prices and delays.

The location of data centres and landing points for submarine cables are in close relations. Places where several submarine cables land ("hubs" for submarine cables) are very adequate for locating data centres, processing data coming from several countries, and the location of data centres is a key factor to consider when selecting landing points. The investment done by large CAPs in submarine cables is coordinated with the deployment of data centres for their own use, and the irruption of large CAPs in the deployment and ownership of submarine cables has implied a shift from cable topologies connecting cities to topologies more focused on connecting data centres, that are the main requirement for large CAPs[135]. This is in general beneficial for Europe in terms of investment, as well as data sovereignty, as more data is stored and processed in Europe rather than in third countries.

Large CAPs' (and other actors') investments in submarine cables tend to have a positive impact on engineering innovations and to push the boundaries for technical efficiency, contributing to lower latency and improved bandwidth and reliability. For example, new submarine cable systems are equipped with technology that allows for faster and cheaper information exchange, which ultimately lowers purchasing price per Tbit/s. The new cable systems also enhance protection through the marine installation and burial tools, which better protect these systems. In summary, the large investments made by some large CAPs have had a positive impact on innovation.

6. Case study 3: Internet relay services

Internet relay services can be considered as a sort of enhanced Virtual Private Networks (VPNs). VPNs exist in different forms and with different characteristics. In general, they build on top of existing networks and can provide a secure communications mechanism for data and IP information transmitted between networks.[136] The set-up of a VPN often depends on the purpose.

An early and still very relevant purpose of VPNs is the connection of multiple sites: companies use VPNs to create their closed (private) network environment where the infrastructure, network management and applications are dedicated to a closed set of subscribers in their also closed corporate environment. For example, the devices of mobile working employees connect via the VPN to this closed corporate environment using public and untrusted networks like the internet. Another purpose of VPNs is to increase the level of privacy of existing internet

[135] Submarine telecoms forum Industry report 2023-2024, see: https://subtelforum.com/industry-report/
[136] NIST SP 800-113, see: https://csrc.nist.gov/glossary/term/virtual_private_network

connections by adding a layer of encryption (in form of an encrypted tunnel) to reduce the possibilities of eavesdropping for sections of the data transmission. VPNs often use some form of endpoint address translation, which leads to the next purpose of obfuscation of the own identity or location. VPNs and internet relay services share the function to increase the privacy, e.g. by obfuscating the own identity. There is no single solution covering all demands. VPNs exist in multiple variations and can be set up on several layers: Link Layer, Network Layer or Application Layer. Each way to reach the abovementioned demands introduces certain costs to consider. An alternative to using the internet via a VPN today is to lease circuits, or similar dedicated communications services, from the public network operators, and create a completely private network.[137] This consists of direct payments for the leased lines, but also of the personnel and expertise to manage the infrastructure, network and applications. To prevent those costs, it is common to use the connectivity of the internet, and set up the VPN on top of this at the application layer. Even when business users contract leased lines to connect their premises, they contract a VPN on top of these leased lines at a higher layer.

To provide a protected information system link, VPNs utilise tunnelling, security controls and endpoint address translation.[138] The encrypted tunnel provides for secure data transmission over untrusted networks. This attribute of tunnelling makes VPNs a suitable tool for connecting multiple trusted sites and devices over untrusted networks like the internet. For example, in corporate environments VPNs connect laptops or smartphones with the internal company network, even when those devices use untrusted environments like public hotspots or while working from home. This has led to enterprise VPN solutions for this specific use-case. The endpoint address translation allows users to obfuscate their own location to prevent some forms of tracking or to access content usually not available in their current location. For this use-case, a separate set of VPN providers is active on this market.

While some of such VPN providers declare a no-log policy in their privacy statements, the VPN provider can still technically view the data traffic. Recently, the possibility for VPN providers to build profiles of their users based on analytics of the data traffic was addressed by several developments, leading to enhancements of those VPN services and similar “internet relay services”. The Internet Engineering Task Force (IETF) has started working on “Multiplexed Application Substrate over QUIC Encryption (masque)” in 2020[139], whose protocols are used for example in some CAP’s internet relay services, such as Apple’s iCloud Private Relay service[140]. Google has developed a similar – however technically different – solution for the Google One VPN service.[141] Another example is the Microsoft Edge Secure Network which is a built-in VPN service in Microsoft’s Edge Browser.[142] All of these internet relay services have in common that the data traffic can technically neither be viewed/decrypted

[137] «What is a VPN?», Paul Ferguson and Geoff Huston, April 1998
[138] CNSSI 4009-2015, see: https://csrc.nist.gov/glossary/term/virtual_private_network,
[139] See: https://datatracker.ietf.org/wg/masque/about/
[140] See: https://www.apple.com/icloud/docs/iCloud_Private_Relay_Overview_Dec2021.pdf
[141] See: https://one.google.com/about/vpn/howitworks
[142]See: https://techcommunity.microsoft.com/t5/articles/introducing-microsoft-edge-secure-network/m-p/3367243/page/2

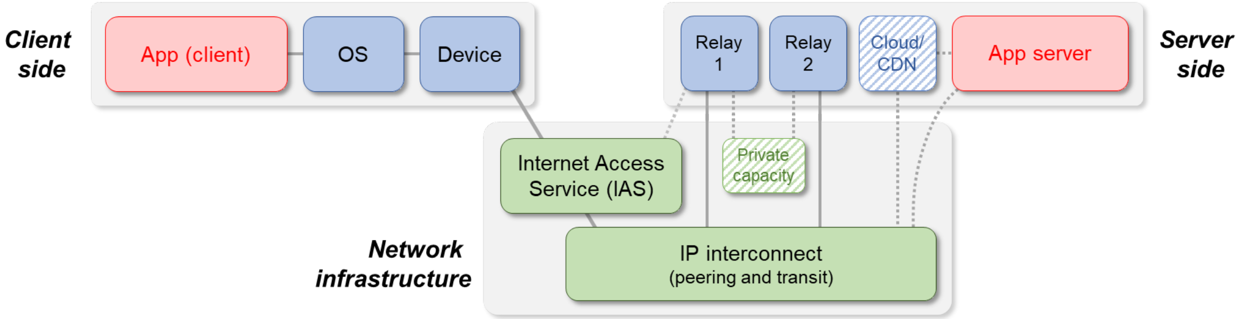
by the relay service providers, nor the content be assigned to individual users of the internet relay service. With this, neither the relay service provider, nor the ISP technically can track or analyse the users' data traffic.

6.1. Description of the service

Technically, internet relay services provided by CAPs work like traditional VPN services: a "tunnel" is established from clients' endpoint (via the clients' existing internet access) to an "entry server" (relay #1) where the user-authentication is checked. All or certain data traffic is transported through a tunnel and reaches the internet after exiting a second "exit server" (relay #2).[143]

The data traffic through this tunnel is encrypted, so that the internet access provider and other network operators between the clients' device and relay #2 have no insight into this data traffic. At relay #1, the user is authenticated and authorised to use the internet relay service. The data traffic is then not immediately forwarded to the internet (as it is the case with traditional VPN services), but after the authentication the data traffic is first transferred to relay #2 where it gets decrypted and can reach the original destination on the Internet afterwards.

Figure 10. Generic overview of the functioning of internet relay services



Legend*: Green** *boxes represent the connectivity segments/services;* ***Blue *boxes represent the hardware and software from the device or cloud server;* ***Red*** *boxes represent the client-server application that is being used.*

Source: BEREC

By splitting the tasks of a single (VPN) server to different servers/institutions (i.e. relay #1 and relay #2), the following characteristics result: the provider of relay #1 can be responsible for managing user access and authentication while not directly handling cryptographic keys and

[143] Descriptions by Apple, About iCloud Private Relay - Apple Support, see: https://support.apple.com/en-us/102602, Google, see: https://one.google.com/about/vpn/howitworks and Microsoft, see: https://techcommunity.microsoft.com/t5/articles/introducing-microsoft-edge-secure-network/m-p/3367243/page/2 in conjunction with Claudflare, see: https://www.cloudflare.com/de-de/microsoft/microsoft-edge-privacy-notice/

thus not being able to decrypt the users' traffic. In this case, the provider of relay #2 is responsible for managing the decryption of the data traffic to forward it to the destination, but relay #2 is not aware from which specific user this traffic comes from. Thus, relay #1 only knows which user wants to transfer data without knowing the content or the destination of this data, and relay #2 only knows the destination and the content of the data (as long as this is not additionally encrypted) but does not know from which user this data comes from. It should however be noted that cryptographic keys are stored in the user's device/VPN-App/web-browser, whose provider can also be the provider of relay #1.

Traffic transported via internet relay services does not show the actual IP address which is assigned by the internet access provider to a user, but the IP addresses of the relay #2-Provider. However, the source IP address is still supposed to indicate the "rough location of the client" (i.e. terminal device), accurate to the users' region or country.[144]

6.2. Business models

There is no common or single VPN business model due to the very diverse use-cases of VPNs explained before. On the one hand, VPNs are used to connect enterprise sites. In the case of leased lines, large investments in physical infrastructure by a network operator is necessary, so the physical connection of enterprise sites on the link layer can be considered separately here. The connection of enterprise sites at the application layer via VPN application can also be considered separately with regard to this use case in the enterprise context. On the other hand, a use case exists for private users to increase the level of data protection in conjunction with the concealment of their own location by using encryption technologies and address translation.

Internet relay services aim at this last use case and typically follow subscription-based business models. Several commercial providers of such services exist and offer subscriptions for access to their VPN-service for monthly or yearly payment. There are also free and open-source solutions fulfilling the same use-case, e.g. "The Onion Router" (TOR), but they do not follow a specific business-model. TOR is available as free and open-source software without any payments, only donations and the support of foundations secure the funding.

The internet relay services provided by the largest CAPs use the following business models (as of January 2024):

- Apple iCloud Private Relay is part of the subscription-based service "iCloud+". Only subscribers of iCloud+ can activate and use iCloud Private Relay, and it works only

[144] iCloud Private Relay Overview, Chapter "IP Address, Identity and Location", see: https://www.apple.com/icloud/docs/iCloud_Private_Relay_Overview_Dec2021.pdf

with iOS/macOS-devices and when using Safari. iCloud+ costs 0.99 euros per month and goes up to 59.99 euros per month.[145]

- The service offered by Google is part of the subscription-based service “Google One”. Only subscribers of Google One can use the Internet relay service by Google One on their Android, iOS, Windows, and Mac devices. Google One costs 1.99 euros per month or 19.99 euros per year and goes up to 9.99 euros per month or 99.99 euros per year.[146] The Google One VPN is also included in any Google Pixel 8 Smartphone for the first 6 month.[147]

- Microsoft Edge Secure Network is built in the web-browser Edge and is free to use for users who signed in with their (cost-free) Microsoft-Account, with an allowance of 5 GB data traffic per month.

6.3. Relations among the main stakeholders involved

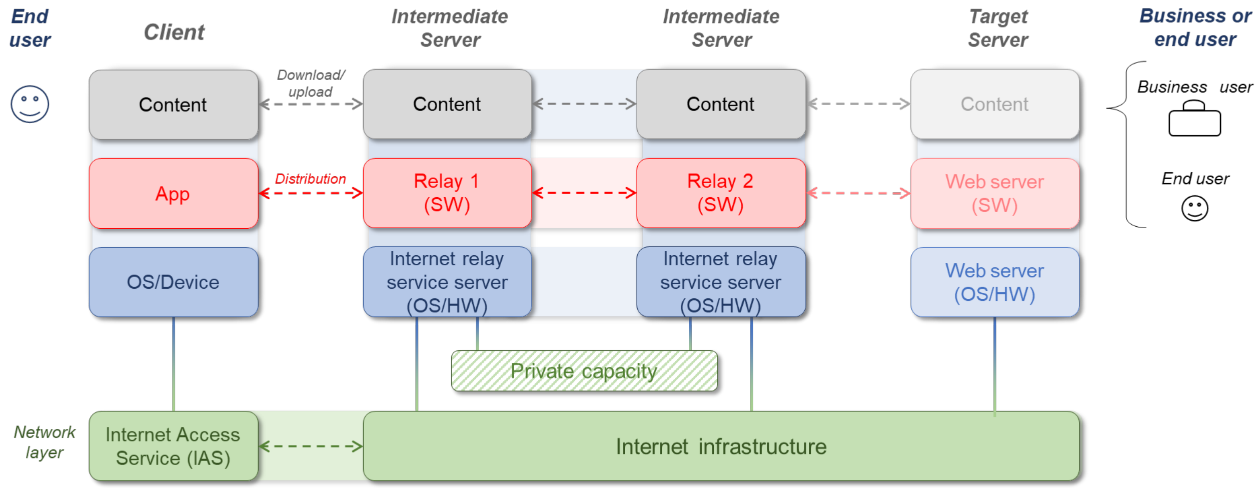
Figure 11 shows the elements and relations of internet relay services within the internet ecosystem. In general, the internet relay service is implemented on the application layer of end-users’ devices – either as a stand-alone app or included in the OS or web-browser. The app gets authenticated by relay #1, and afterwards the encrypted data traffic goes through relay #2 where it gets decrypted and forwarded to the original destination (target server).

The CAP cannot see the users’ IP-address and eventually a precise network-based location anymore. However, authentication of the single user by other means than the IP-address is still possible (e.g. via an account of the user with the target service). And it is also still possible to locate the user by other means (e.g. precise location via GNSS of the device).

From the internet access providers’ view, the use of internet relay service affects the provision of the IAS to the customers in a way that the network-dimensioning and interconnection-agreements may need to be reconsidered and also the ability of the IAS provider to analyse its customers behaviour based on traffic analysis.

[145] See: https://support.apple.com/en-us/HT201238
[146] See: https://one.google.com/about/plans
[147] See: https://store.google.com/de/product/pixel_8

Figure 11. Relations between users, CAPs, IAS providers and internet relay services



***Legend**: **Green** boxes represent the connectivity segments/services; **Blue** boxes represent the hardware and software from the device or cloud server; **Red** boxes represent the client-server application that is being used.*

Source: BEREC

Internet relay service differ from traditional VPN services in several ways. In most cases, the provider of traditional VPNs can access and analyse the data traffic. In the case of enterprise VPNs, it is in the intention of the company for example to filter the internet traffic and prevent the transmission of malicious software. However, with internet relay services which split the data traffic between two entities running the two relay servers, it is more difficult for the operator of relay #1 to gain any insight of the data traffic and the operator of relay #2 cannot associate the traffic with any user. With this split, the use-case of an enterprise VPN cannot be fulfilled by internet relay services. Enterprise VPNs and internet relay services aim at different markets and are not in competition to each other.

VPN services can also be used to obfuscate the users' location and allow them to get access to location-restricted content. Internet relay services could not be used for this purpose since a rough location would still be provided. Therefore, such services are not substitutes of, and not competing with, VPN services in this use case.

6.4. First insights on the service

VPN and internet relay services are typically used to ensure confidentiality by encrypting the data traffic directly on the users' devices or in the users' domain. This can affect internet access providers and other actors in several ways, some of which are analysed here below. The list is not meant to be exhaustive.

6.4.1. Traffic identification and management

When users make use of a private relay or VPN service, Internet access providers can still identify the origin and the destination on an individual basis for data transport in order to reliably route data packets to and from their users. However, insight into the content of the data traffic is technically no longer possible, since the data traffic is transported through the encrypted tunnel (and it is important to note that such deep packet inspection is legally not allowed for the ISP). The (public and un-encrypted) IP addresses in the data packets can also still be viewed, both by the internet access provider and by other network operators.

This means that services based on user identification (e.g. self-service portals) remain possible only when the identification is done on the application layer, not on the network layer anymore. This is also true for the case of a web browser-based use: the browser-based access of websites which rely on network-based identification information will no longer be possible since browser' data traffic is transmitted through the tunnel and therefore cannot be identified and charged by the internet access provider.

However, in principle, VPN or internet relay services do not make it more difficult to use and control the network efficiently, since the data traffic would be concentrated towards the VPN/relay service providers, and all traffic originally transported to different destinations and interconnection points now can be transported to the interconnection towards the VPN/relay service provider. Nevertheless, these changes of traffic flow certainly lead to changes in the utilization of an internet access providers' current interconnections in case the number of users of internet relay service will significantly increase, and this may have implications for its network topography. In such a case, the internet access provider would have to re-negotiate existing interconnection agreements or set up new interconnection agreements to fulfil their customers' demands of high-quality connections to the providers of internet relay services (i.e. currently the large CAPs Apple, Google and Microsoft). Against this background, internet relay services may *ceteris paribus* imply a certain shift of relative bargaining power towards CAPs that provide such services, as well as a shift concerning which connections are prioritised or developed.[148]

6.4.2. ECS operators' services (self-service portal, payment, speed tests)

As explained above, users cannot be identified by the internet access provider based on network-related information anymore when any form of VPN is used. Thus, the use of payment services or self-service portals which are based on IP traffic identification may have to be adapted to other means of user identification (e.g. by web access authentication with usernames and passwords, public-key authentication, token-based authentication or credentials stored on a SIM).

[148] It should be noted that internet relay services are just *one* factor impacting on the relative bargaining power between the parties involved.

Speed tests can – from a technical point of view – continue to work but the results may be misleading. Indeed, when activated, the internet relay services and other internet infrastructure are included in the measurement results, thus making the result about the IAS flawed and not meaningful anymore due to a lack of assignment. This can be avoided if the users of a speed test are explicitly advised/required to deactivate VPN or internet relay services during the measurement.

6.4.3. Network security and privacy

The security and resilience of networks is not compromised by transmitting encrypted traffic. The task of an internet access provider is to transport data, regardless of the type, content or quantity of the data.

As noted above, when internet relay services are activated, it is still possible to identify users and to differentiate traffic categories when separate treatment is necessary (for example in case of specialised services). However, ECS providers cannot read or influence their customers' data traffic anymore due to their use of encryption, such that internet access providers can no longer block certain destinations/websites for their users.

However, lawful interception is still possible, where internet access providers are able to intercept communications data. This data can be provided to the authorities only in encrypted form, as opposed to clear text. This encrypted format provided to authorities is not just the case for internet relay services or VPNs, but is the norm generally, due to a trend towards higher demands in relation to the citizens' privacy and the increasing use of encryption on different layers and in more and more applications.

6.4.4. Impact on traffic concentration and innovation

Internet relay services are made possible by innovative transport protocols such as QUIC and represent a contribution to increasing data security and privacy. However, it should be noted that data traffic is concentrated to a single destination which is controlled by large CAPs at the moment. While other enhanced VPN providers can offer such internet relay services, large CAPs may have a competitive advantage since users use closely related services (e.g. web browsers or operating systems) of such CAPs. In some cases, the internet relay services by large CAPs may even be exclusively bundled with other software of the CAP. This may lead to a bigger lock-in effect and an additional manifestation of the market position of the large CAP, since users may stick to the CAPs ecosystem and do not switch to other – maybe better fitting – providers.

The impact of internet relay services on online advertising and, in particular, on digital services whose business model relies on users' data monetisation, should also be considered, especially when these services are provided by the actors which could compete with the CAPs proposing internet relay services.

Finally, the concentration of traffic to few internet relay service providers might also lead to a devaluation of many small interconnections, while positively affecting the reachability of the large CAPs since the interconnections with them need to be upgraded and prepared.[149]

7. Restrictions on access to services or functionalities by OS providers

Recent technological developments and specific services provided by large CAPs – and in particular by providers of OS – can sometimes restrict ECS/ECN providers' ability to correctly provide access to services or to the network. The potential concerns mentioned in this chapter relate to the elements in the internet ecosystem that are mainly controlled by large CAPs and BEREC is exploring these issues given their potential impact on competition and investment for ECS.

The examples below are based on stakeholders' feedback received by BEREC and NRAs in the last years. Therefore, they are not meant to be exhaustive and sometimes concern only *potential* issues.

7.1. OS & key features for the provision of access services

Over the last years, regulators have been made increasingly aware of issues involving operators and some device manufacturers and OS providers concerning the access to essential features of devices.

In particular, such issues may involve the configuration of technical settings for core features supported by the network and device typically related to the provisioning of ECS, such as voice, messaging and data services[150]. GSMA has published some recommendations[151] on a framework for device manufacturers/OS providers and MNOs to assist them to configure devices and ensure they can support services offered by the MNO. However, these customisation packages are deployed using a mechanism under the control of the device manufacturer/OS provider (while the deployment of such a mechanism is out of scope of GSMA Recommendations), which may raise challenges for some operators.

[149] The issue of IP-interconnection will be analysed in the "BEREC Report on the IP interconnection ecosystem", to be approved in 2024. BoR (23) 210, BEREC Work Programme 2024, 07.12.2023, see: https://www.berec.europa.eu/system/files/2023-12/Work-Programme-2024.pdf

[150] It should be noted that the issues described do not relate to applications layer customisations including deployment of MNO specific apps, UI (User Interface) customisation and branding assets.

[151] The configurations would typically take place upon first insertion of a SIM by a process called "Late Customization". Refer to GSMA Recommendation published in May 2022 "Technical Adaptation of Devices Through Late Customization" Version 11.0, see: https://www.gsma.com/newsroom/wp-content/uploads//TS.32-v11.0.pdf

For instance, MVNOs have often highlighted[152] through their association MVNO Europe that major device manufacturers and/or OS providers are not making some key features of their devices, necessary for the provisioning of APN-related services (data traffic, MMS, mobile hotspots), the provisioning of IMS-based services (VoLTE, VoWiFi, specific messaging services such as visual voice mail) or even 5G access available to MVNOs. According to these MVNOs, the concerned manufacturers are either blocking or have made no efforts to ensure (after specific requests from MVNOs) that these features correctly work with every operator's profile, in the absence of a carrier partner agreement with the manufacturer. Carrier partner agreements seem to be often unavailable or not suitable for smaller operators (both MNOs and MVNOs, as they also encompass, for example, large-scale sales agreements). As a consequence, these operators face issues in setting up all functionalities of the devices. In some cases, MVNOs report that they maintain two different infrastructures (light and full-MVNO) just to be able to get access to the carrier profile of their hosts as a light MVNO; this situation could imply an additional burden to the business model of these actors, which in many cases are relatively smaller market players.

7.2. OS & eSIM

Whereas the usage of SIM cards has enabled a seamless functioning between operators (whether they are MNOs or MVNOs) and handset manufacturers, the adoption of eSIM and iSIM enables the device manufacturer or OS provider to be in control of the network profiles loaded onto its devices. Hence, operators not identified by the device manufacturer have difficulties setting up their network profile on the corresponding devices chosen by their end users. The forecasted adoption of eSIM and iSIM as a standard for many types of connected devices can be a source of concern, given the fact that manufacturers could choose to restrict to some extent the number of compatible network profiles and seek to prioritise commercial partnerships in their carrier agreement policy.

This situation could have consequences on the market dynamics of ECS services and the ability to freely choose and switch between telecommunication operators.[153]

[152] BoR PC12 (22) 08, Contribution of MVNO Europe contribution to the public consultation on the Draft BEREC Report on the Internet Ecosystem, 22.07.2022, see: https://www.berec.europa.eu/en/document-categories/berec/public-consultations/contribution-of-mvno-europe-to-the-public-consultation-on-the-draft-berec-report-on-the-internet-ecosystem

as well as BoR PC04 (21) 10, Contribution by MVNO Europe contribution to the public consultation on the BEREC Draft Report on the ex-ante regulation of digital gatekeepers, 04.05.2021, see: https://www.berec.europa.eu/en/document-categories/berec/public-consultations/contribution-by-mvno-europe-to-the-public-consultation-on-the-berec-draft-report-on-the-ex-ante-regulation-of-digital-gatekeepers

[153] BoR (23) 41, Study on wholesale connectivity, trends and issues for emerging mobile technologies and deployments, 13.04.2023, see: https://www.berec.europa.eu/en/document-categories/berec/reports/study-on-wholesale-mobile-connectivity-trends-and-issues-for-emerging-mobile-technologies-and-deployments

7.3. OS & slicing

Network slices provide end-to-end logical networks to different industries/users allowing customization, dedication, and isolation of network resources. As far as the deployment of 5G network slicing functionalities is concerned, some operators identify potential issues in their relation to manufacturers, and more precisely OS providers. To correctly identify and transmit traffic according to the specifications of the slices put in place by operators, an interaction between the network and the device is necessary. This interaction is materialized through the UE Route Selection Policy (URSP) rule matching logic, that determines which URSP rules, if any, match an application as specified by 3GPP standards.

The OS provider plays a special role in this context. This is due to the fact that the routing of the application to the slice depends on the OS of the end-user, and in some situations the operator has to apply a configuration designed by the OS provider to connect the application and the slice. This configuration is specific to the OS provider and not directly linked to 3GPP standards, because schematically the signal goes through the following steps: app->OS->modem->network; only the interface between modem and network is based on 3GPP standards. Therefore, in such situations[154]**Error! Bookmark not defined.** the OS determines how the device, as well as applications on the device access the slice, which means that operators cannot control the slice from end to end, in particular regarding the consistency of the QoS for each application. It should be noted that the GSMA has set up a task force within its Terminal Steering Group aimed to facilitate operator and vendor alignment in order to discuss how such gaps could be fulfilled besides other issues where the user's device might be involved in the provisioning of network slicing (including authentication and authorization mechanisms for network slicing).

Given the concentration of the consumer market for device OS[155], there is a risk that major OS providers are in a position to impose de facto standardisation to the slicing identification mechanism and that as an effect, operators may lose part of the control over which traffic corresponds to each slice. This evolution has to be monitored with the principle of Open Internet in mind, as there could be issues related to the free choice of the device by the users and the respect of reasonable traffic management. Also, as a consequence, this lack of control could mean that value generating possibilities for operators concerning slicing may be limited, despite slicing and differentiation possibilities being identified as one of the potential levers for new business models on a 5G SA network.

The control of the network operator over the provisioning of the slices, as well as over the identification mechanism, does not pre-empt the type of offers that can be provided over the

[154] This is the case when App ID and OS ID are used as entries for the traffic descriptor to determine whether a URSP rule matches or not.

[155] As stated in BEREC's Report BoR (22) 167 on the Internet Ecosystem, the mobile OS market in Europe is mainly split between Android (63.6% market share by 2022) and iOS (35.7%)

network, and it does also not prevent the end-users from having a control over the applications and the slices they want to use.

Similar questions arise concerning material that is used by private 5G networks (e.g. for industrial purposes). Clients of such solutions might find themselves confronted to limitations when using equipment of some vendors and OS providers that have not foreseen, or sometimes banned, the use of their equipment in the configuration of a private network. This limits the availability of suitable equipment for 5G private networks, which is *per se* an issue on the market, and inhibits the development of hybrid solutions based on private and public networks.

7.4. OS & Rich Communication Services

Rich Communication Services (RCS) is a standard of messaging meant to replace traditional SMS with new and more interactive features, especially multimedia transmission. When using RSC, end-to-end connectivity must be ensured, as mandated by Article 97 EECC.

The original standard for RCS was developed by the GSMA between 2008 and 2016. Following the publication of specifications known as the "universal profile" in 2016, the implementation of RCS has been supported by several MNOs, OEMs and CAPs. Among those, the implementation of RCS within the messaging services of the Android OS (*Messages* by Google) has led to quick uptake, as it was gradually rolled out as a default feature of this OS.

To use RCS, the OS needs to enable it and partnerships must be available on equal terms with all ISPs.

Even though end-users had to opt in to use the Android RCS in its first years of existence, the fact that it was the only RCS app available, and a native messaging app installed on the device, resulted in a quick uptake of this provider-specific solution. The uptake might accelerate again as Google announced in August 2023[156] that RCS would be enabled by default (and an opt-out option) for new and existing Android users (provided they use a compatible device and MNO carrier profile).

Notwithstanding, take up of MNO-specific RCS solutions, based on upgraded standards developed by the GSMA, including developments on technical and commercial interoperability between providers, seems to be ending[157]. In this context, it may be useful to monitor if the

[156] See: https://support.google.com/messages/thread/229405182/your-rcs-conversations-are-now-fully-end-to-end-encrypted?hl=en&sjid=12459911091064889808-EU

[157] Vodafone waves goodbye to RCS, shifts over to Google (lightreading.com), see: https://www.lightreading.com/services/vodafone-waves-goodbye-to-rcs-shifts-over-to-google; RCS discontinuation & alternatives – Help | Swisscom, see: https://www.swisscom.ch/en/residential/help/mobile/rcs.html;
Verizon, AT&T, T-Mobile kill RCS plans (lightreading.com), see: https://www.lightreading.com/broadband/verizon-at-t-t-mobile-kill-rcs-plans

choice between RCS providers exist and can be made in an easy, explicit way, and if interoperability between different types of providers can be promoted or enforced. The implementation of the DMA might be relevant in that regard.

Some additional issues that BEREC also considers as useful to be explored:

- Legal obligations (e.g. legal interceptions): it is important to verify if the same standard of obligations can be applied to RCS services. For example, there is currently no guarantee that legal interceptions can be performed on RCS services, especially when they are provided by a CAP.

- Transparency towards operators on the statistics of usage of these services: when the RCS platform is provided by a CAP, ECS operators can lose their vision of the actual usage of these services and be unable to have up to date statistics.

- Availability of Google RCS services for every ECS operator profile (also MVNOs or smaller operators): currently, RCS services provided by Google are rolled out (and made available to the end-users) on the basis of agreements with each of the ISPs on the market, and smaller operators should have access to the RCS platform on the same terms.

- Cross platform interoperability: in the current form of the roll-out of RCS services, interoperability is not taken for granted. If RCS as a standard becomes a popular alternative to traditional texting, it can be detrimental to have end-users unable to reach users on other RCS platforms. Unlike other typical instant messaging services, end-users are not able to install by themselves competing RCS solutions if these have not been rolled out on their ISPs network.

- Availability and use of RCS on Apple devices: Apple's iMessage messaging app also tends to replace traditional operator messaging services as the default communication canal between two Apple devices. Apple devices do not support the RCS standard that could compete with iMessage. However, Apple announced in November 2023[158] that it would enable the RCS standard on its devices in 2024. At the time of writing of this report, it has yet to be confirmed how apps based on the RCS standard will work alongside iMessage, which seems to remain the default messaging solution for Apple devices.

It deserves to be noted that, while RCS are ECS, the elements of the device or the software that are concerned by the potential restrictions mentioned here above do not fall within the regulatory scope of BEREC members under the EECC.

[158] See: https://9to5mac.com/2023/11/16/apple-rcs-coming-to-iphone/

OSs are core platform services under the Digital Markets Act, and BEREC will keep monitoring the evolution of the OS providers' practices in light of the application of the DMA obligations in order to tackle the impact on ECS/ECN regulation.

Table 2. Overview of a selection of current/potential restrictions on access to services or functionalities by OS providers

Effect	Potential issues	Possible implications
OS -> MNO/MVNO	Specific partner agreement needed for MNO/MVNOs to configure APN related service	Data traffic, MMS or mobile hotspots are unavailable for customers of the concerned operator and device manufacturer
OS -> MNO/MVNO	Specific partner agreement needed for MNO/MVNOs to configure IMS related services	VoLTE, VoWiFi, messaging services are unavailable for customers of the concerned operator and device manufacturer
Device manufacturer or OS -> MNO/MVNO	Difficulty in setting up the network profile of an MNO/MVNO in the absence of a preloaded network profile on an eSIM or iSIM	Customers of the concerned operator are unable to use the equipment linked to the eSIM or iSIM
OS-> device manufacturer or MNO	Potential predominance of OS on the authentication and authorization mechanisms for network slicing	Difficulties to make network slicing work accordingly to the plans and provisions of the MNO, potential transparency problem for traffic management and possible limitation in choice of equipment for the end-user
OS -> competing RCS applications and traditional messaging services	Predominance of OS-backed RCS app	Difficulty or impossibility to install competing apps, migration of traditional ECS usage towards the OS backed solution

8. Conclusions

Large CAPs have traditionally provided services on the client and server sides of the internet ecosystem. However, in recent years, they have increasingly invested in network infrastructure and provided services related to ECN and ECS, or qualifying as such.

This report provides an overview of the impact of large CAPs on the markets for ECN and ECS in Europe. BEREC has already highlighted[159] how the accumulation of a significant variety of the internet ecosystem elements in the hand of a few Big Tech companies can have important consequences, such as leading to market concentration (as it is the case e.g. for

[159] BoR (22) 167, BEREC Report on the Internet Ecosystem, see: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-internet-ecosystem.

cloud services, instant messaging, and OS), or affecting internet traffic and the decentralised approach on which the internet was created.

In order to better analyse the implications of the CAPs' presence and strategies in ECS/ECN markets, three case studies focusing on CDNs, submarine cables and internet relay services, are carried out.

The commercial CDN services market in Europe currently appears to be concentrated around few players, as significant investments are required to have the necessary geographical coverage and capillarity to enter the market. Such concentration is expected to grow significantly in the coming years. Previously, large CAPs relied on commercial CDNs providers for their services, but in recent years they have been increasingly rolling out their own CDN infrastructure networks. They mostly use it for self-provision but also partly provide CDN services to third-parties, thus directly competing with commercial CDN providers. Moreover, on the one hand, the roll-out of CDNs by large CAPs – often on the ISP's network (i.e. on-net CDN) – exerts competitive pressure on the business model of transit providers; while on the other hand, on-net CDNs allow to reduce cooperatively capacity costs for ISPs by locating content closer to end-users.

The submarine cable ecosystem and the relations among stakeholders have significantly evolved in the last few years: large CAPs have transformed from mere direct or indirect customers of wholesale capacity, to the owners and investors in transport network infrastructure. They have become the driving force behind a significant portion of newly-deployed high-capacity systems: they are currently responsible for more than 60% of the international traffic transits through submarine cables and are able to lease capacity on some of their cables to the ECN/ECS providers. In this context, while large CAPs deploy submarine cables primary for their own use, traditional ECS/ECN providers still play a key role on the transmission of data for other CAPs, connecting areas which may not be economically profitable. Moreover, by primarily interconnecting their data centres and regional PoPs to data centres, large CAPs' investments have limited impact on the global network resilience.

Many large CAPs also provide internet relay services, which are used to ensure confidentiality by encrypting the data traffic directly on the users' devices or in the users' domain. The report analyses the potential impact on internet access providers. Lawful interception still appears to be possible, where internet access providers are able to intercept communications data. Moreover, in principle, such services do not make it more difficult to use and control the network efficiently, but changes in the traffic flow impacts on the utilisation of an internet access providers' current interconnections, as well as on the decentralised approach of the internet architecture. Finally, as far as users' confidentiality of data is concerned, it should be noted that cryptographic keys are stored in the user's device/VPN-App/web-browser.

Furthermore, BEREC is aware of some potential issues which deserve to be further analysed to evaluate their impact on the ECS markets. Indeed, recent technological developments and specific services provided by large CAPs (and in particular by OS providers) can sometimes restrict ECN/ECS providers' ability to correctly give access to services or to the network itself.

Typical examples include the access to 5G slicing functionalities or other restrictions to the provision of the slices, the potential implications of provider-specific solutions for standardised services (e.g. RCS), as well as the difficulties that some MVNOs and smaller mobile operators seem to face in setting up some functionalities of the devices (e.g. APN-related services, VoLTE, VoWiFi) or in configuring the network profile when eSIMs are used.

To sum up, BEREC's analysis highlights how large CAPs insource what was formerly purchased from traditional ECN/ECS providers to a large degree. Indeed, large CAPs have deployed their own physical infrastructure, such as CDNs and data centres, as well as network infrastructure, such as submarine cables. By building their own large autonomous systems, they rely to a significantly less extent, or not at all, on long-distance transit provided by ECN/ECS operators. Simultaneously, they also impact the overall network topography, e.g. by creating direct connections to data centres or incentivising the prioritisation of high-quality connections to particular sites.

The relations between large CAPs and ECS/ECN operators can take several forms: i) CAPs and ECS/ECN operators offer complementary services, which mutually increase each other's demand (e.g. operators providing broadband internet access services and CAPs provide content and applications; the devices and OS by large CAPs being sold together with an operator's bundle offer; set-top boxes integrating both access to the internet and to OTT services or to voice assistants), and ii) several cooperation partnerships between ECS providers and CAPs can be observed at the national level. However, these actors are also iii) direct competitors, as it is the case for e.g. voice and messaging services, video-streaming content platforms vs. linear television and IPTV, cloud service provision, CDNs, submarine cables, as well as for access networks such as LEO satellites, 5G private networks for businesses, and, in some non-European countries, fibre networks.

This report highlights several issues which can raise some challenges in the context of ECS/ECN regulation, and which could be further investigated by BEREC in the future. In order to carry out evidence and fact-based analyses, BEREC stresses the need to collect relevant data from the actors who can have an impact on the ECS/ECN markets which are regulated. The EECC revision provides an opportunity to adapt the regulatory framework and ensure that the current or potential issues can be correctly tackled.

9. Future work

In line with BEREC's strategic priority to support competitive, sustainable and open digital markets[160], BEREC will keep monitoring and analysing the markets that may be significantly impacted by the digital players.

[160] BoR (23) 48, BEREC Action Plan for 2030, 09.03.2023, see: https://www.berec.europa.eu/en/document-categories/berec/others/berec-action-plan-for-2030.

This report highlights some topics which BEREC could further investigate in the future. This is for instance the case for the increasing investment of CAPs in data centres in Europe and their impact on the provision of ECN/ECS.

Moreover, building on the “Study to Monitor Connectivity-Connecting the EU to its partners through submarine cables” prepared by PwC for the EC in July 2021, BEREC could update the information on submarine cables capacity and resilience for Europe, and provide a detailed overview of the level of congestion and resiliency of the routes in each country. In this line, it could also be interesting to analyse: i) different EU maritime areas (e.g., Atlantic, Baltic, Mediterranean Sea); ii) the direct connectivity between the EU and Latin America (in collaboration with Regulatel), the direct connectivity between the EU and Africa; iii) the international and national connection for island countries (e.g. Cyprus, Iceland, Ireland or Malta) and islands/archipelagos in other countries, or maritime connections for close countries through the sea (for example, Finland and Estonia).

Further analysis on the issues raised by the MVNOs associations on potential restrictions imposed by OS providers would also be interesting. This could be done by means of questionnaires, interviews or workshops with MVNOs, OS providers and consumer associations. The potential effects on IoT could also be explored.

Furthermore, the impact of large digital ecosystems on business communications services (usually bundled with other services such as cloud and software) and the implications for the ECS providers could be further explored.

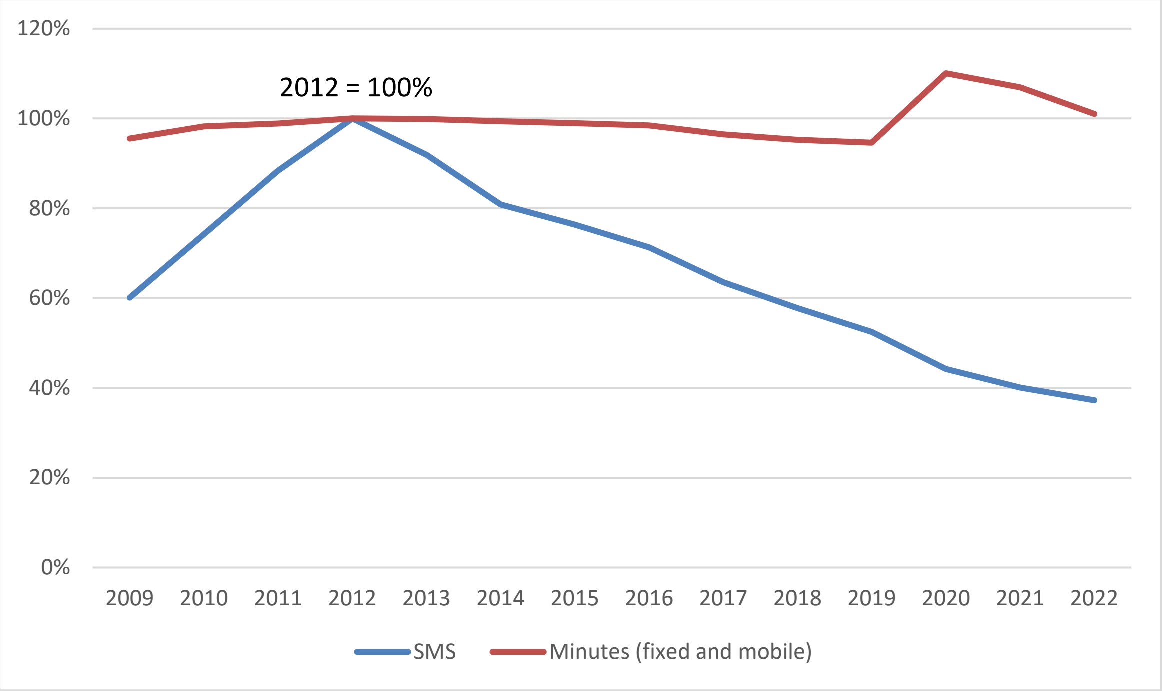
In order to carry out evidence- and fact-based analyses, BEREC stresses the need to collect relevant data from the actors who can have an impact on the ECS/ECN markets which are regulated by its members. BEREC believes that its data-collection powers would deserve to be reinforced in the context of the EECC revision. Such revision may also be the opportunity to clarify the qualification of some services/network which are very closely related to the ECS/ECN.

Finally, BEREC will continue to collaborate with the EU institutions, both for the implementation of the Digital Markets Act and the Data Act, as well as any other regulatory instruments for elements in the internet ecosystem.

Annex 1: Evolution of voice and SMS as compared to 2012

The graph in Figure 12 compares call minutes (adding both fixed and mobile call minutes) and SMS volumes from 2009 to 2022 with regards to their respective level in 2012. It is based on data from 19 European countries,[161] adding up the volumes of minutes and SMS across these countries. In total, SMS increased until 2012 and then dropped while call minutes remained fairly stable (with an increase in the pandemic period).

Figure 12. Evolution of call minutes and SMS volumes from 2009 to 2022, as compared to 2012



Minutes based on data from 19 countries: Austria, Bulgaria, Croatia, Czech Republic, Denmark, Finland, France, Germany, Greece, Liechtenstein, Luxembourg, Malta, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Spain

SMS based on data from 19 countries: Austria, Bulgaria, Croatia, Czech Republic, Finland, France, Germany, Ireland, Italy, Greece, Liechtenstein, Luxembourg, Malta, Norway, Portugal, Romania, Serbia, Slovenia, Spain

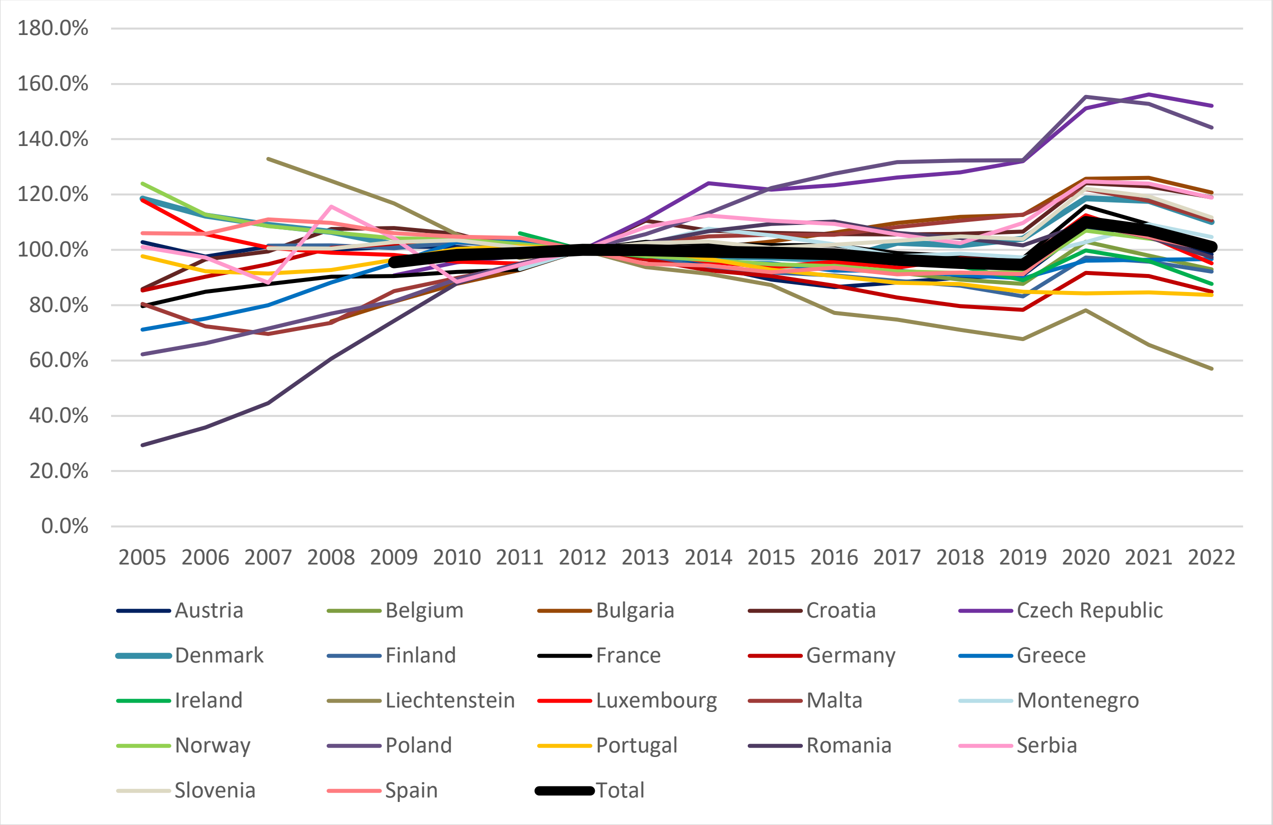
Source: From BEREC data collection

Figure 13 and Figure 14 show that the trends are different across countries. The line "Total" is the same as in Figure 12. In addition to the countries listed in Figure 12, some other countries were added, for which data were not available over the entire period 2009-2022.

[161] The list of countries differs between minutes and SMS.

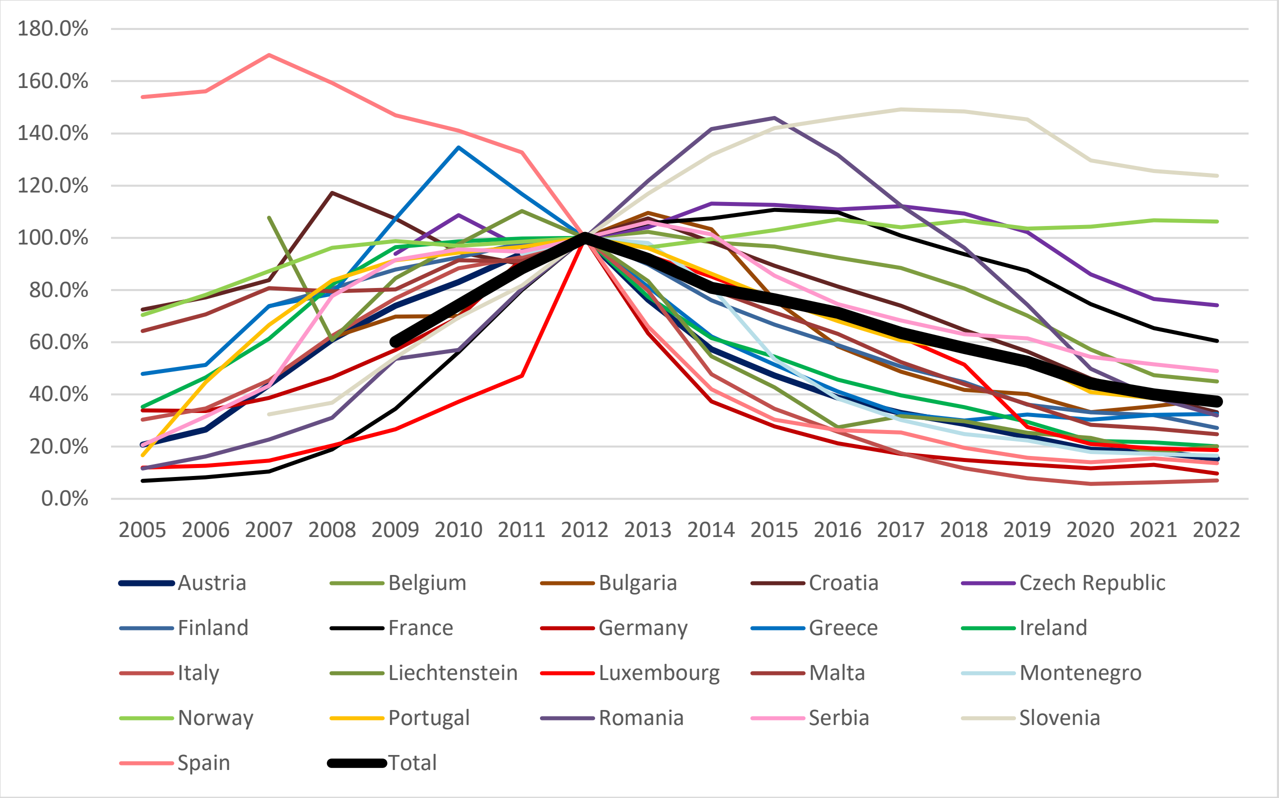
These countries are Belgium, Ireland, and Montenegro for call minutes and Belgium, Montenegro for SMS.

Figure 13. Evolution of call minutes volume from 2005 to 2022, with regards to 2012 level



Source: From BEREC data collection

Figure 14. Evolution of exchanged SMS volume from 2005 to 2022, with regards to 2012 level



Source: From BEREC data collection

Annex 2: List of abbreviations

API	Application Programming Interface
BEREC	Body of European Regulators for Electronic Communications
CAP	Content and Application Provider
CDN	Content Delivery Networks
CPS	Core Platform Service
DMA	Digital Markets Act
DSA	Digital Service Act
EC	European Commission
ECN	Electronic Communications Network
ECS	Electronic Communications Services
EECC	European Electronic Communications Code
ETSI	European Telecommunications Standards Institute
IAS	Internet Access Service
ICS	Interpersonal Communication Services
ISP	Internet Service Provider
ITU	International Telecommunication Union
NI-ICS	Number-Independent Interpersonal Communication Services
NRA	National Regulatory Authorities
OS	Operating System
OTT	Over-the-top
PoPs	Points of Presence
PPP	Public Private Partnerships
SMS	Short Message Service
VPN	Virtual Private Network

Annex 3: List of figures and tables