BoR (23) 208

Study on the trends and cloudification, virtualization, and softwarization in telecommunications

Report prepared for BEREC by Plum Consulting and Stratix

7 December 2023

This document has been prepared for the Body of European Regulators for Electronic Communications (BEREC). However, it reflects the views only of the authors, and BEREC cannot be held responsible for any use which may be made of the information contained therein.

The study was undertaken by

plum

and

Stratix

Authors: Dr Aude Schoentgen (Plum), Chris Taylor (Plum), Rudolf Van Der Berg (Stratix)
The study team included: Sarongrat Wongsaroj (Plum), Karim Bensassi-Nour (Plum), Bart Garvelink (Stratix), Paul Brand (Stratix)

Contents

Executive Summary

The Study

In this report we document the findings of our research in the project undertaken for BEREC by Plum Consulting and Stratix on the technology trends, market and business developments and impacts on competition and regulation of cloudification, virtualization and softwarization in telecommunications.

The objectives of this assignment were:

1. to research and report on the technical evolution of electronic communications networks and services;
2. to conduct market and business research and analysis;
3. to identify, research and report on use case studies;
4. to analyse business dynamics and future trends; and
5. to analyse and report on impacts and potential impacts on competition and regulation.

The Deliverables for the project have been organised in two stages. A report was delivered to BEREC covering items 1 – 3 listed above in August 2023. We have combined that work with items 4 and 5 to produce this integrated report.

The approach to this exploratory study utilized a mixed methodology, combining desk research and stakeholder interviews. More than 20 interviews enabled us to assess our initial findings against the experiences and expertise of stakeholders, to get their real-world insights, and help disentangle hype from reality.

The findings

Technology evolution

The report describes the evolution from vertically integrated service-specific network architectures through the growth of IP networks to current ecosystems in which network and service functions which were previously reliant on dedicated physical resources have been moved into virtual environments where they are controlled by software. These functions are increasingly hosted in private or public cloud environments.

This evolution has been facilitated by some notable technology developments. These include:

- **Virtualization**. Virtualization allows network functions and resources to be delivered independent of hardware as virtual networks.

- **Containerisation**. Containerisation is a way to combine software coding with necessary data and other dependencies so that it can run on any platform.

- **Software Defined Networking (SDN)**. SDN enables the functions of a network to be controlled by software. It has therefore removed the previous close integration between network hardware and network functions.

- **Network Function Virtualization (NFV)**. NFV is a type of virtualization in Electronic Communications Networks (ECNs). It provides virtualization of network functions meaning they can be shared in the physical network by a number of services. Therefore, network functions are no longer physically located.

- **Cloudification**. Cloudification is the hosting of data and compute in data centres. In electronic communications, cloudification has enabled virtualised network functions to be hosted in this way.

These developments have been significant in the evolution of ECNs for the delivery of both fixed and mobile Electronic Communications Services (ECSs). They have significantly changed the dynamics of networks, and improved efficiency through easier scalability, better reliability and resilience, flexibility, and higher utilisation.

The research identified the following technical trends:

- **Evolution models**. Virtualization of core network functions allows operators to manage core network functions in the cloud, using either dedicated SDN Telco Cloud infrastructure or virtual private networks on public clouds.

- **Developmental issues**. There are various models of cloud deployment in the ECN/ECS value chain. Brownfield deployments often take a phased, risk-based approach, starting with lower-risk OSS and BSS systems before integrating into core or access network architecture. The development of Open RAN has given rise to complexities in integration because of the disaggregation of RAN components and vendors. As Open RAN and other complex ecosystems evolve, automation becomes important for effective deployment, while the transformation also necessitates a shift in skill sets, emphasizing software and programming, over traditional engineering skills.

- **Testing**. Effective testing is essential when deploying new technologies like Open RAN. Deutsche Telekom's O-RAN Town trial was an important step in Open RAN validation, and from this Deutsche Telekom was able to document and report learnings, including on system integration and multiple vendor compatibility.[1] Open RAN requires compatibility testing among vendors, prompting open-source platforms for preliminary testing. Organizations like the O-RAN Alliance offer integration facilities, while automation enhances the testing process's efficiency and risk management.
- **Standardisation**. Standards play a crucial role in electronic communications, promoting interoperability and system integration, as exemplified by the GSM standard. However, as technology evolves, there is a challenge in aligning the rapid pace of innovation with the establishment of standards. Efforts from organizations like the O-RAN Alliance and ETSI aim to develop industry standards, with stakeholders emphasizing the need for open, global standards that foster innovation while preventing fragmented standard development.
- **Security**. Network evolution and service provision introduce cybersecurity risks that necessitate consistent security measures across technology platforms. Disaggregated software and vendor architectures, coupled with shared infrastructure, pose challenges in security coordination, emphasizing the importance of robust access control. ECN operators prioritize security in planning cloud-based, softwarized, and virtualized solutions, ensuring compliance with varying jurisdictional requirements, while vendors recognize the market's demand for secure solutions.
- **Environmental sustainability**. The transition to software-based, virtualized, and cloud-based ECNs has potential environmental benefits, including more efficient data storage, reduced physical infrastructure, and lowered energy consumption. Despite the anticipated positive environmental impact of such advancements, research and stakeholder discussions indicate that the actual relationship between network cloudification and environmental benefits is not yet fully assessed.

[1] See https://www.telekom.com/en/company/details/bundled-in-a-white-book-learnings-from-o-ran-town-1026846

Impact on business dynamics and competition

Alongside this technology evolution, the cloud market landscape is changing business dynamics in ways which affect both regulated markets and other areas of CSP activity. For example:

- **CSPs have embarked on a digital transformation driven by technical evolution**. CSPs are undergoing a digital transformation, utilizing cloud-based solutions to modernize operations and enhance customer experience, with a focus on flexible, scalable, and cost-effective network management. This transformation sees CSPs transitioning from traditional network architecture to a software development approach, emphasizing advanced analytics and AI. Whilst this is evident across all CSP facets, it is particularly pronounced in network provision, management, and support systems, with the COVID-19 pandemic having further accelerated the demand for improved capacity and resilience.

- **CSPs are adopting a cautious "wait and see" approach in some cases.** CSPs have exhibited caution in their approach to digital transformation due to technical, financial, and operational challenges. There can be concerns about network reliability, interoperability between vendor components, financial overheads of transitioning, and the need for upskilling personnel. As cloudification and other technologies shift the landscape, relationships between CSPs and traditional vendors are evolving, with some CSPs taking a more in-house approach. Despite the potential for greater agility and breaking free from vendor lock-in, interoperability and standardization remain significant hurdles.

- **CSPs are exploring new business models but face uncertainty**. The technology evolution described in this study has created risks to CSP core revenue streams, but also opportunities for them to diversify and build new business models. Among related challenges, the migration of networks and support solutions to the cloud means that CSPs need to move customised legacy applications to the cloud while maintaining service continuity.

- **Hyperscalers have an increasing and multifaceted role**. Hyperscalers are playing diverse roles in the telecom value chain, ranging from partners to competitors. They've established partnerships with telecom software vendors like Amdocs and Netcracker to bring services to the cloud, providing cost efficiencies and scalability. Additionally, they act as intermediaries, offering platforms like AWS Marketplace for vendors to reach CSPs more easily. However, hyperscalers like AWS and Microsoft are also entering domains traditionally occupied by CSPs, such as private networks. Direct investments, like Google's in Jio Platforms, show their evolving influence in telecoms. Despite the potential benefits of partnering with global platforms, CSPs remain cautious about over-dependency on hyperscalers, striving for more standard and open solutions.

- **Vendor diversification**. A consequence of the technical evolution identified in this study has been the diversification of the cloud ecosystem, with a variety of suppliers and vendors providing facilities and services to CSPs, making the landscape more complex.
- **Open APIs**. The transition has also ushered in an era of more open systems, with APIs and their levels of openness playing a notable role in this evolution of the ECN/S value chain. API openness in the electronic communications sector introduces significant advantages as well as challenges across the value chain in cloudified and virtualised environments.
- **Interoperability and standardisation**. This is important to competition. A relevant risk is that a lack of openness and standardisation will foreclose market entry opportunities for smaller players and favour those who can provide multiple solutions within a locked ecosystem. Hence, technical barriers may disproportionately impact smaller competitors, potentially further boosting the influence of global players who can leverage their inherent competitive advantages.

In essence, the technical transformation in ECN/S, led predominantly by cloudification, is reshaping the industry. From the diversification of the cloud ecosystem to the emergence of new technical barriers, the implications are manifold and varied. How different segments of the industry respond to these challenges will have an influence on ECN/S market dynamics.

Impacts on regulation

The study considered the impact of the technical evolution and changes in business dynamics on the regulatory landscape for Electronic Communications Networks and Services (ECN/S).

The supply of ECN/S in Europe is regulated under a well-established system which has been successful in delivering effective competition and good consumer outcomes in Europe. However, the technology evolution described in this report (cloudification, virtualization and softwarization) has contributed to an environment in which ECN/S are capable of delivering a wide variety of digital content and services that are not regulated within the ECN/S framework.

This has also created a complex value chain. To understand the challenges raised by these technology developments and to ensure markets and consumers are safeguarded therefore requires collaboration between regulatory authorities, policy makers and other stakeholders.

We have identified the following areas in which electronic communications regulators will continue to play an important role, sometimes alongside and in collaboration with other responsible authorities.

- **Competition in vendor markets**. Changes in upstream vendor markets, for example, the development of disaggregated provision of RAN components has the potential to diversify the ECN/S supply chain. This may improve competitive intensity. However, complex supply chains are potentially risky. For example, Open RAN disaggregation introduces new challenges in testing and integration and hence new risks in the ECN/S value chain. These risks may also affect investment. Standardisation and testing can mitigate this.

- **Competition in adjacent markets**. ECN/S markets are affected by influential players in adjacent or related markets. This report describes how hyperscalers are active in a number of ways in the ECN/S value chain. Regulators and competition authorities have recently conducted studies of the cloud market, and will wish to continue to monitor developments in cloud markets.

- **Impact of global scale on smaller markets and operators**. Economies of scale in the trend to multinational and global solutions in virtualized networks may make it more difficult for smaller operators and smaller jurisdictions to develop bespoke solutions or forge bespoke vendor relationships for their markets and consumers.

- **Investment**. Regulators have an interest in ensuring there are not barriers to efficient investment in connectivity and access. This may involve continued monitoring of the technology landscape and upcoming developments to ensure that this does not create risks, for example to ensure appropriate arrangements are in place for the robust testing and sometimes standardisation needed to deliver complex new systems.

- **Potential for digital exclusion**. There is a risk that innovation and development of new services delivers benefit to some users whilst others are excluded, for example because of the affordability of new services or devices. This is a common feature of technology evolution. Regulators have a role to promote digital engagement.

- **Security of networks and data**. New technology can affect the security of networks and data. Networks, vendors and regulators are working to eliminate or mitigate incremental risks.

- **Environmental impact**. Technology evolution also affects the environmental impact of the provision of ECN/S. More efficient solutions have improved this impact relative to previous network architectures. However, there are also environmental costs arising from the deployment of new infrastructure and increased demand for some facilities and services. Electronic communications regulators, operators and other stakeholders are increasingly focussed on initiatives to further improve the environmental impact of the sector.

The trends analysed in this study are dynamic, and continued study and analysis by regulators is appropriate.

1. Introduction

Cloud services have become increasingly important in many sectors. According to Synergy Research[2], the value of the public cloud services and infrastructure market totalled USD544bn in 2022 with 21% Year-on-Year (YoY) growth. In the telecom sector, the growing use of cloud services and cloud computing in the context of Electronic Communications Services (ECS) provision has been the catalyst of a number of fundamental developments in network technologies, including Software-Defined Networking (SDN) and Network Functions Virtualization (NFV). NFV and SDN have been deployed in both fixed and mobile architectures, but they are particularly relevant in the context of 5G networks which have been designed to fully exploit the benefits of the cloud. Open RAN solutions which are emerging in 5G are software-based solutions that make use of open and modular Radio Access Network interfaces. This makes it possible for hardware and software components provided by multiple suppliers to be integrated into one overall solution, and virtualization and cloudification enable network operators to run software services from multiple vendors on generic hardware.

While these technical developments are still in their early stage, the telecommunication industry is witnessing a paradigm shift that is affecting the ECS provision value chain. The traditional model of ECS provision characterised by proprietary hardware and software network equipment and on-premises software solutions, is becoming more complex and more dynamic as a result of cloudification, virtualization and a general pattern of software run on commodity hardware replacing dedicated hardware.

Traditional suppliers such as equipment vendors and software providers have evolved to adapt to the new market requirements, and new players have also emerged. The new model of ECS provision relies on a complex ecosystem comprising traditional ECS providers, cloud infrastructure and services providers, traditional equipment vendors and cloud-native software vendors and integrators. Partnerships are being forged between the different players and market dynamics are more complex as players are involved in different parts of the value chain.

The aim of this report is to describe the current technical and market trends in the provisioning of ECN/S that stem from the cloudification of network elements, and to analyse the potential regulatory issues it could raise. The report is structured as follows:

- Section 2 provides an overview of our approach and methodology
- Section 3 provides a description of the traditional ECN/S (Electronic Communications Networks/Services) model
- Section 4 provides a definition of key concepts related to virtualization and cloudification

[2] https://www.srgresearch.com/articles/total-public-cloud-revenues-jumped-21-in-2022-surpassing-500-billion-despite-economic-headwinds

- Section 5 provides a description of how the traditional ECN/S model is evolving
- Section 6 provides practical considerations for the deployment of these technologies
- Section 7 sets out an overview of the technical trends related to the deployment of these technologies
- Section 8 assesses the impacts of these technical evolution on the market dynamics, and
- Section 9 discusses the potential challenges for regulation.

Annexes of the report include, among other elements, three use cases as well as a list of complementary recent sources of information on cloud markets.

2. Our approach and methodology

The approach to this exploratory study utilized a mixed methodology, combining desk research and stakeholder interviews. In our desk research, various sources have been covered extensively, including regulatory and policy documents, government reports, commercial offers, market research reports, white papers, and other publicly available resources. The interviews enabled us to assess our initial findings against the experiences and expertise of stakeholders, and to get their real-world insights.

The main challenges we encountered in our desk research are:

- Disentangling hype from reality: Some of the key concepts and technologies covered in this study are still at an early stage of commercialization and even technical development. This means that much of the publicly available information about these technologies comes from promotional or marketing perspectives, and it was therefore important to identify empirical evidence where it is available.

- Inconsistent information about key concepts: Some of the key concepts and technologies covered in this study have not yet been formally defined or standardized. This means that definitions and conceptualization are not aligned across different sources. To avoid any confusion, we provide a definition of key concepts and technologies covered in our study.

We conducted more than 20 interviews with key market players, encompassing telecommunications service providers of varying sizes, equipment vendors, cloud providers, and the public sector. These interviews served as a complementary research method to validate the key findings derived from the desk research and address the two challenges discussed above. Appendix A shows the list of companies we have interviewed for this first stage of the project, and Appendix B lists the questions we used as guidance for the interviews.[3]

It is important to note that these interviews were conducted in accordance with the Chatham House rule, which guarantees the confidentiality of the participants, and helped us to get additional insights from experts. According to this rule, participants are free to use the information shared during the interviews, but they are prohibited from disclosing the identities or affiliations of the speakers or any other participants.[4] Key learnings and findings from these interviews have been identified and reflected in the report, without disclosing the sources.

[3] Note that not all the questions listed were covered in each interview, and interviewees sometimes wanted to raise different points, which they were free to do.

[4] http://www.chathamhouse.org.uk/about/chathamhouserule/

3. The traditional ECN/S model

This chapter gives an overview of a traditional value chain for Electronic Communications Networks and Services (ECN/S). By contrasting the traditional model with the model that emerges when cloud, NFV and SDN are deployed, we will then show in the following sections where and how the provision of ECN/S is changing.

3.1 Historical background

The telecommunications value chain refers to the various activities and processes as well as the different roles and players that are involved in creating and delivering ECN/S to customers. The ECN/S value chain used to be service specific and distinguished between different customer types and applications. Therefore, there were separate value chains for fixed and mobile networks which distinguished between consumer and business customers, between voice and data, national and international, etc.

In the 1980s and 1990s it became increasingly clear to the industry that digital technologies enabled networks to be layered. This would allow the same infrastructure using ATM (Asynchronous Transfer Mode) and ISDN (Integrated Services Digital Network) to carry multiple service types and for different types of customers.[5] Initially, changes happened under the direction of the telecommunications company who would provide all these services, and the manufacturers that supplied them. The assumption was that a uniform infrastructure would support the different services and applications. It was envisioned that there would be different service classes with characteristics, such as low latency, guaranteed bandwidth or best effort optimised for different types of applications and services. The network would recognize the type of application and associated service classes and provide the required technical characteristics and quality of service that were optimal for the application or service. Such a network was characterised as an “intelligent” network.

The breakthrough of the Internet from 1994 from academic networks disrupted this model, and IP became the basis of global networks around the world. They were built as a federation of interconnected networks who had a loose set of agreements on how IP packets should work and how routing was done using the Border Gateway Protocol. Instead of a few telecom companies, there were now hundreds if not thousands of independent networks known as autonomous systems in each country. Neither the equipment nor the network operator needed knowledge of the types of services used and deployed over the network. This allowed for rapid and permissionless innovation, the type of network is sometimes characterized as a service-agnostic network (or “stupid” network[6]), that offers the same class of service for each service.

[5] The OSI-layer model was a result of these ideas and guided the way firms thought the market would develop.

[6] A seminal paper that described the difference between the two approaches is “Rise of the Stupid Network”, David Isenberg Computer Telephony, August 1997, pg 16-26, which can be found at https://dl.acm.org/doi/pdf/10.1145/280437.280445

All these developments raised a question: if IP-networks weren't built around a telecom network operator, who could define what services were available on the network?

The move to IP-based networks first happened in fixed networks after 2000. BT in the UK was one of the first traditional telecom firms to publicly state that it would build its networks around IP technologies. BT envisioned Ethernet as the basis of its network even though Ethernet did not have a background as a standard for telecom-grade networks (it had been used for local-area-networks and then datacentres and wide area networks). Compared to ATM-based networks it was considerably cheaper to implement but didn't have all the features that were thought to be necessary for telecom-grade networks. Ethernet and IP quickly progressed to become the basis of the Internet and the digital ecosystem as we know it today.

In mobile networks the existing tight integration of networks and services remained in the following years. It was not until the definitions of 4G and particularly 5G that they began to be separated. When 3G was defined, the Internet was only just becoming a mass market medium. When 4G was developed it was clear that IP would be the basis for mobile networks, but how this could be achieved was still unknown. 5G standardization aims to make IP the basis for mobile networks, and so 5G networks can benefit from IP network innovations that have developed over the last two decades.

At the same time, the ever-increasing demand for services over the Internet pushed the development of what is now known as “the cloud” or “hyperscale datacentres”. Delivering services over the Internet meant that users with connectivity to a network could be anywhere in the world, and if a service became popular, there quickly might be millions of users in countries around the world. Amazon was one of the first companies to realize that the engineering challenges it faced when scaling its computing and networks for online shopping were the same challenges that other online merchants and service providers would face at some later point. In 2002 it launched “Amazon.com Web Services” as one of the first generic cloud platforms.

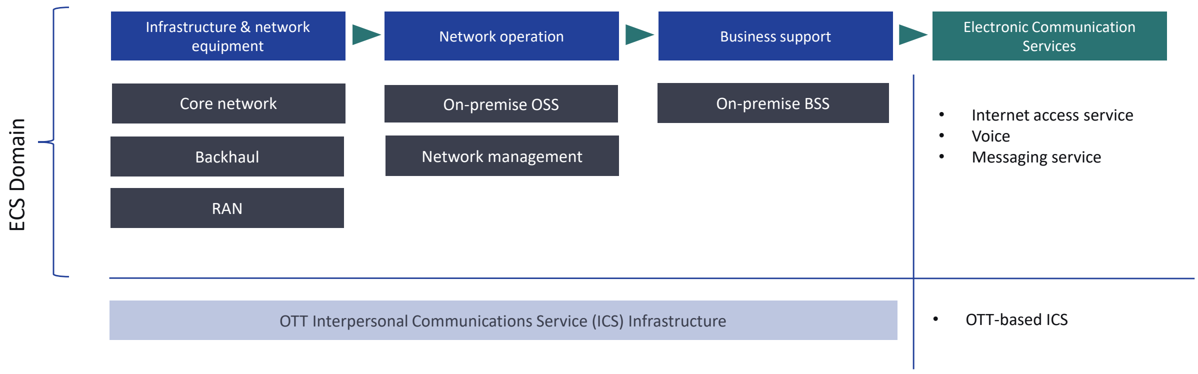
Telecom firms were built on more traditional monolithic architectures for their services, billing and operational support using mainframes and server architecture specific to a group of products and services. The complexity of billing, service plans and the types of services and quality parameters specific to customers created a rigid integration of the different components of the ECN/S value chain. In recent years, telecoms providers have been able and willing to look at telco cloud solutions for network operation and management, and for internal processes.

3.2 Components of the traditional ECN/S value chain

Figure 3.1 shows the different components (grey boxes) of each element of the value chain in a traditional model for ECS provision. In the traditional model each of these services had its own infrastructure and network equipment, with its own network operations (operational support systems (OSSs) and network management systems) and business support systems

(BSSs). These would be there for telephony, for business data services, fixed and mobile network provision. These components are a mixture of hardware and integrated software as well as operating functions that are key to value creation in each layer in the traditional model. The output of the value chain is the delivery of ECS, including internet access service, voice and messaging services.

Figure 3.1: Components of the traditional mobile ECN/S value chain



3.2.1 The traditional value chain in fixed networks

We illustrate this with the example of fixed network telephony. Historically, there was a separated telephony network for analogue voice. Digitisation of the core of the network in the 1980s and 90s was specific to just the voice service. There was a specific network operation function for voice that was supported by OSS to monitor how well the service delivery functioned. The specific parameters that were relevant for each customer would be set in the BSS. For an organisation with multiple locations, the BSS would provide the OSS with the necessary information to deliver a call (e.g. numbers in use and locations information). There was tight integration between these systems to make sure the network delivered what was agreed in the contract (e.g. nationwide the same phone numbers and 4-digit dialling for internal calls, bandwidth allocation and traffic classes). In many cases, the billing was service parameter specific (e.g. internal calls not being billed despite the callers being in two different cities), which meant that the various options had to be represented in the billing system. Offering a large corporate customer a single number for its call centre (or local numbers that would all terminate in a single call centre) would require each element to be represented in each of the parts of the value chain and the relevant systems.

3.2.2 The traditional value chain in mobile networks

In mobile services, the network infrastructure facilitates communications with devices. It can identify the location of devices, which antennas need to service which device, how handover between cell sites is done, and which frequencies devices will use for different types of applications and services. It adds and removes encryption on the signal, measures the quality of connections and shifts traffic so that performance is maintained even though there are variable factors in the network (e.g. the number of active users). These systems and processes ensure that the bits that are sent and received for the different services are processed correctly, and the user doesn't lose connection.

The network operations elements provide authentication functions to ensure only validated customers can make use of the network. This involves a Home Location Register (HLR) for the network's own customers, and a Visited Location Register (VLR) for inbound roaming customers. It authenticates the SIM-card and verifies the user subscription status. It enables value added services for specific customers or gives certain types of customers priority. It includes the mobile switching centre and IP-routing functionality to make sure that calls and data packets flow between customers or to other networks. It also generates the billing data that is needed for business support. It is common for MNOs to outsource the management of network operations to manufacturers such as Ericsson, Nokia and Huawei. In the case of a single vendor managing multiple operator networks, these operator networks would all be strictly segregated.

The BSS perform many different functions. A major element is subscriber management which includes the subscriber data, the subscription types they have and the value-added services that are part of how the service is offered (e.g. how many minutes, SMS, unlimited, roaming included or not etc.). This is the basis for the OSS and for the billing system that keeps account of the users' credit, bills according to usage and processes payments. Business support also gives the various departments of a telecom firm insight into how the network and business is operating. BSS were among the first parts of the network that saw virtualization "as a service" offers and cloudification, where MNOs didn't manage the hardware and/or software they needed, but instead outsourced this to a third party. This meant that increasingly the data and processes of different mobile networks would run in the same business support system operated by their supplier.

The tight integration between each component of the value chain has decreased over time in fixed networks but is still very present in mobile networks. There are a number of reasons for this:

1. Mobile networks are standardised in generations and the requirements of 2G and 3G were integrated across the various components of the value chain. 4G allowed some separation of functionality, but still required close integration for some services such as voice. 5G is the first generation to take full advantage of the possibilities of virtualization.

2. Mobile networks need to support inbound and outbound roaming with other networks. The roaming devices depend on certain services to function in a common way across the components of the value chain.[7]

[7] Roaming for Voice over LTE posed various problems for operators, because the integration of various components was not as tightly standardised. Security requirements were operators specific. The solution that was found, was to route VoLTE voice back to the home operator instead of handling it locally as is done for 2G and 3G voice.

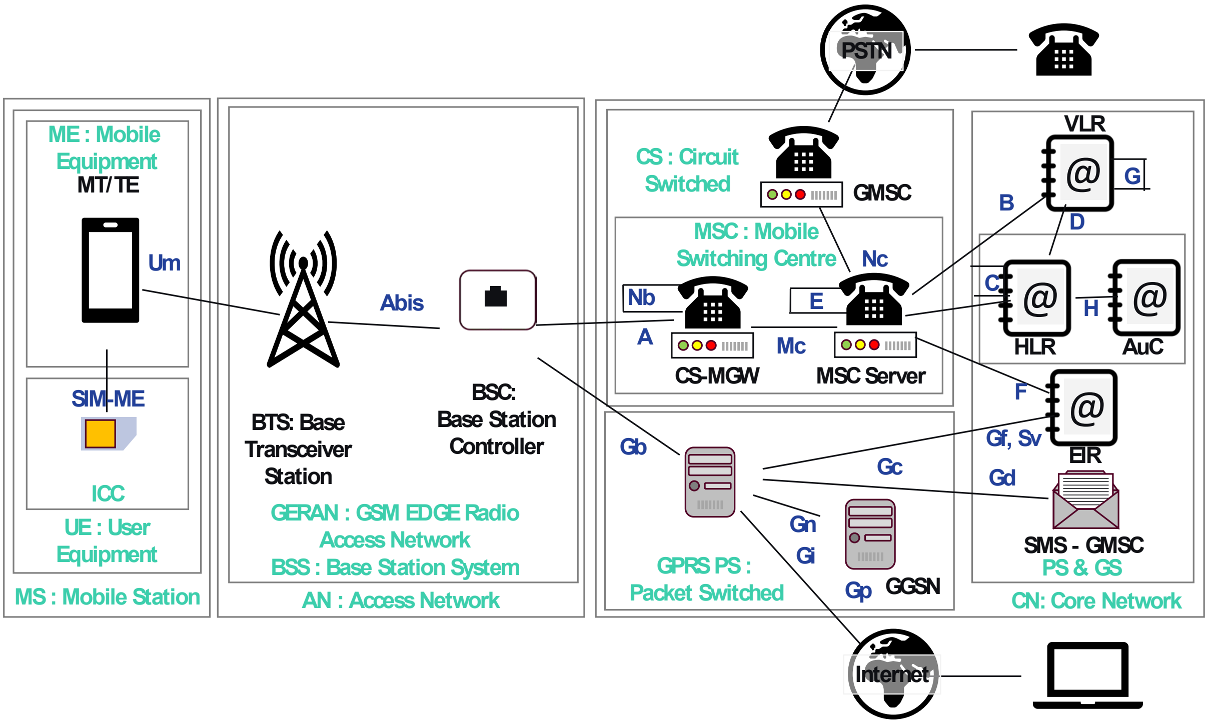
3. The radios and baseband units are tightly integrated in 2G, 3G and 4G, meaning they are typically supplied by a single manufacturer.

As a result, in the traditional value chain it is challenging for operators to benefit from cloudification, SDN, and NFV, whether implemented separately or together in an offering such as Open RAN. This explains why, particularly for Open RAN and cloud networks, the first examples were new networks that were deployed as greenfield or near greenfield.

3.3.3 Infrastructure and network equipment[8]

In the traditional 2G/3G networks there was close integration between the antenna site and the core of the network.

Figure 3.2: Structure of a GSM network



Source: Wikimedia commons https://commons.wikimedia.org/wiki/File:Gsm_structures.svg

Radio Access Network (RAN)

The Radio Access Network handles the wireless communication with the user's terminal equipment (e.g. a mobile phone). It consists of a number of elements:

[8] Note about Network design: Network design could be considered as part of Infrastructure and network equipment. but also as part of Network operations when much of the design is using software tools.

- Antennas that convert electrical signals into radio waves and vice versa;
- Radios that change digital information into signals for wireless transmission and ensure that transmission take place over the correct frequency bands and at the right power levels;
- Base Transceiver Station (BTS) or Baseband units (BBUs), that are responsible for signal processing functions that enable wireless communication. Traditionally, baseband uses dedicated electronics along with software to help execute wireless communication over the licensed radio spectrum. BBU processing functions include error detection, securing the wireless signal and ensuring effective use of wireless resources.
- Base Station Controllers (BSC) control a number of BTS/BBU's in such a way that different sites functioned as a complete network, handling interference, handover and coordination between sites.
- The locations are combined into overlapping cells so that the user can move at up to 300kph (as fast as a high-speed train) while maintaining communication. This results in a honeycomb-like structure of the network.

Traditionally the radios and BBUs are bundled together and installed as dedicated equipment at cell sites on an MNO's access network. In a Single RAN network, a multiband, multi-port antenna is combined with several radios. Antennas and the bundled radios and BBUs in 2G/3G and 4G networks are tightly integrated in such a way that it is not possible to use radios from different vendors with different BBUs. The signals that come from the antenna and how to process them is proprietary for each manufacturer. Even though some mobile networks have a multi-vendor strategy, each site is using a single manufacturers equipment for one or more generations of mobile communications.

Backhaul

Backhaul refers to links, consisting of hardware and software, that connect the RAN with the regional network, such as the mobile switching centres (MSCs), or the core. The term MSC is sometimes also used for the connections from several BTS/BBU to the Base Station Controllers. Initially these were 2mbps leased lines or equivalent using copper networks and point-to-point radio connections for sites that didn't have a fixed line. With the increasing capacity needed for 3G and 4G, fibre optic connections replaced copper connections. Physical links such as fibre connections are either self-provided by the MNOs or leased from other telecom networks.[9]

[9] https://www.alliedmarketresearch.com/wireless-backhaul-equipment-market#:~:text=Key%20Developments%2F%20Strategies-,Ceragon%20Networks%2C%20Cisco%2C%20Huawei%20Technologies%20Co.%2C%20Ltd.,wireless%20backhaul%20equipment%20market%20forecast

The requirements on the quality and capacity of backhaul increased with the growing demand in data traffic and the lower latency required to control different RAN locations into a highly performant mobile network. In 4G networks it became possible to coordinate different frequencies to communicate with a device and to coordinate the different RAN locations to manage interference between cells. Whereas in 2G networks adjacent cells wouldn't use the same frequencies, 4G and 5G networks deploy ever more complex methods of coordination between cells. This puts stricter requirements on latency and thereby on the design and topology of networks.

Core network

A mobile core network is located between the RAN and external networks (other telcos' networks or the Internet). It carries out switching functions for all services, which include voice calls, text messages, and mobile data. It also manages packet-switching in 2G, 3G, 4G and 5G networks as well as both circuit and packet-switching in 2G and 3G networks.[10]

With some mobile networks in Europe handling around 1 Terabit/s peak traffic, the core networks are built upon fibre optic links to datacentres where the network operations functions are located. They also interconnect with other networks of the operator, roaming exchanges, and other mobile networks.

3.2.4 Network operations

Operational Support System (OSS)

OSS refers to the information processing systems used by ECN providers to monitor, control, analyse and manage their networks. Traditionally, OSS provided network-facing or network-operations-facing functionality which includes fault and performance management (assurance), customer activations (fulfillment), asset inventory / configuration management, and network security. The information and data generated by OSS are key inputs for planning for overall capital expenditures (CAPEX) and operating expenses (OPEX). As networks grew more complex, OSS capabilities became more sophisticated in terms of performance management, service provisioning and activation, particularly through the integration of network analytics and artificial intelligence.

Network Management

Network Management refers to all maintenance and day-to-day operations conducted on the network. It includes traditional deployment capabilities that cover the rollout of networks from

[10] https://commsbrief.com/what-is-a-mobile-core-network/

site acquisition to acceptance such as project management, site engineering, civil works, installation, and integration.

3.2.5 Business support

In traditional BSS, data is distributed in different data systems repositories[11]. This has evolved with virtualization and cloudification of BSS, and this is explained further in Section 5.1.3.

Business Support System (BSS)

BSS refers to software applications that facilitate all client-facing and business operations of the telecom network. BSS may cover services like billing and invoicing, CRM[12] (Customer Relationship Management), sales and marketing management, financial management, administrative support, HR management, reporting and analytics, Business Intelligence (BI), etc.[13]

BSS supports and delivers a broad range of functions.[14] It brings together sales teams (who contact customers) and engineering teams (who build networks), to initiate revenues (activation flows), retain revenues and customers (assurance flows), collect revenues (billing flows), optimize profitability (efficiencies) and operationalise the assets.

BSS components vary across organizations, depending on business needs and requirements. Depending on the telecom operator's choices or strategy, some services are not included in the BSS portfolio. For instance, in some organisations, financial reporting is not part of BSS.

3.3 Markets for supply of components/services in the traditional model

This section provides an overview of the roles of different types of players.

Figure 3.3 shows the categories of suppliers of the three building blocks of the mobile value chain.

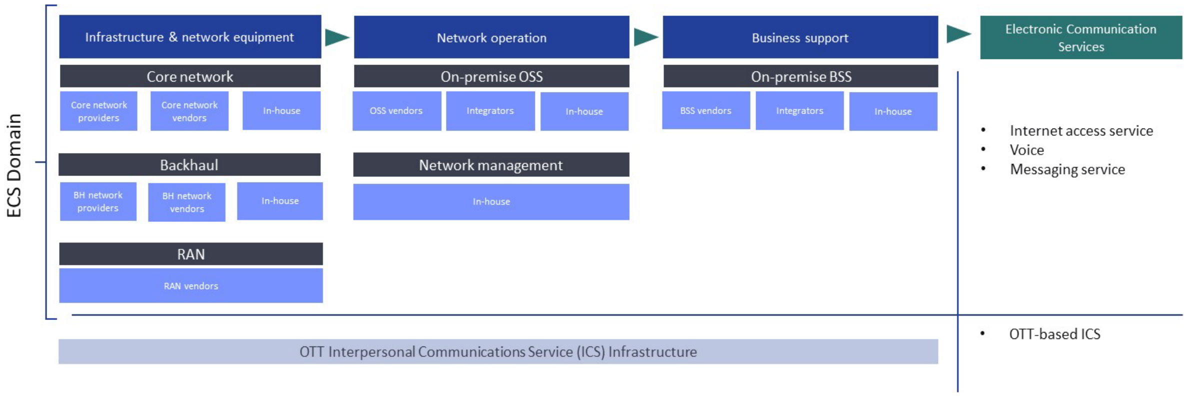
[11] A repository holds data from various sources either in their native format (in which case it is called a data lake) or in transformed format (in which case it is called a data warehouse).

[12] CRM are software tools enabling to manage all interactions and communications with present and future customers, including support and helpdesk services for instance.

[13] https://www.comviva.com/products-solutions/digital-systems/bluemarble/bluemarble-bss

[14] https://passionateaboutoss.com/background/what-are-oss-bss/#chapter1.1

Figure 3.3: Suppliers of the traditional mobile ECN/S value chain



3.3.1 Infrastructure and network equipment

Today, Ericsson, Nokia and Huawei have strong positions in the supply of equipment, software and support across the value chain in Europe. There have been some shifts in the market, because the 5G Toolbox[15] from the European Commission led to a reassessment of vendors in critical parts of the network. Strict standardisation and interoperability made sure that the products manufacturers offered for 2G and 3G had the same functionalities with little room for (proprietary) differentiation in implementation. The result was that mobile network operators could compare the different solutions offered by manufacturers quite well on total cost of ownership. Successful manufacturers were able to achieve economies of scale in their product development and operational support. For 4G and 5G there have been significant differences in deployments between manufacturers and between network operators. The result is that there is much more differentiation between 4G and 5G networks and it is more complex to make devices work across all networks.

In fixed networks the differentiation is less of an issue. The local loop is often operator specific. Local loops can be based on Docsis, DSL, Ethernet, XGS-PON, GPON and various other technologies, depending upon the physical cable type and the type of customer. Backhaul is based on a mixture of fixed connections and wireless (microwave). Transport and core networks are based on fibre optic and ethernet, which is standardised, despite a large number of manufacturers.

[15] For information on the Toolbox see https://op.europa.eu/en/publication-detail/-/publication/7def1c03-da16-11eb-895a-01aa75ed71a1/language-en. The European Commission monitors the Toolbox and its most recent report on implementation can be found here: https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox

Core network

For a telco, the core of its network with the Mobile Switching Centre (or MSC, handling traditional voice services), HLR/VLR and packet gateways is generally a single vendor affair, because it is tightly integrated with how the network performs the various functions to deliver services to the customer. It can be insourced by the operator (Figure 3.3, 'core network'/'in-house') or can be provided by an external provider, either by a 'core network vendor' (Figure 3.3) or by another operator renting the use of their infrastructure (Figure 3.3, 'core network providers').

Backhaul

The supply for backhaul is classified the same way (Figure 3.3). Backhaul equipment vendors have over time migrated to Ethernet-based networks. They include Ceragon Networks, Cisco, Ericsson, Huawei, Juniper Networks, MikroTik, Qorvo, Nokia, Siklu Communication, and ZTE. These companies supply the electronic equipment that is needed to create backhaul links. Where such links rely on physical lines such as fibre connections, the MNO would either build the physical connections themselves or purchase them from another operator.

RAN

For the RAN, some networks chose a dual-vendor approach or purchase different generations of RAN equipment from different manufacturers (Figure 3.3, 'RAN vendors'). Ericsson, Nokia and Huawei have strong positions in this market[16], with smaller market shares for Samsung and ZTE. For specific solutions such as indoor, other manufacturers can play a role such as Airspan, Commscope, Fujitsu and NEC. RAN equipment is tightly integrated between the antenna, BTS and BSC and so a single supplier would be selected by an MNO to roll out its access network using the supplier's proprietary hardware and software solutions.[17] There is debate among market analysts over market shares and revenues of the various manufacturers. Huawei used to have the largest market share and revenue. The exclusion of Huawei from some markets and the restrictions on the supply of high-end chips necessary for 5G RAN antenna mean shifts in the market. Ericsson and Nokia are able to provide the higher end RAN equipment, which has a higher value and have access to markets from which Huawei has been excluded. At the same time China has closed its market, which means that market shares are shifting. The market for this type of equipment is estimated at around 20 billion USD of the total $100 billion USD market size for telecom equipment.[18]

[16] https://telecoms.com/520012/global-ran-market-continues-to-stagnate/
[17] https://omdia.tech.informa.com/OM023522/Market-Landscape-RAN-Vendors-2022
[18] https://www.fiercewireless.com/wireless/who-leads-global-ran-market-ericsson-says-mobile-experts

Figure 3.4: RAN revenue ranking, 2022

	Global	China	Excluding China
Rank #1	Huawei	Huawei	Ericsson
Rank #2	Ericsson	ZTE	Nokia
Rank #3	Nokia	Ericsson	Huawei
Rank #4	ZTE	Datang Mobile	Samsung
Rank #5	Samsung	Nokia	ZTE

Source: Dell'Oro Group, 2023

Some suppliers are active in the supply of RAN, backhaul and core. These are Ericsson, Nokia and Huawei[19]. These are all large integrated vendors that supply proprietary equipment for mobile networks (hardware and software) for all parts of a telco's network. Others, such as Juniper and Qorvo, appear to be focused on equipment for transmission, including switches and routers.

3.3.2 Network operations

In the traditional model, OSS solutions were mainly on-premises software solutions. This means that telecom operators would purchase a license or a copy of the software to use it on their own physical location. Integrators such as Capgemini or Atos were often involved in the integration of the different IT solutions into the operator's environment.

The implementation of OSS solutions is done through a variety of methods which include the following (Figure 3.3):

OSS vendors

These are developed by specialised OSS vendors such as Nokia, ZTE or Ericsson. These vendors focus on building comprehensive OSS platforms that cater to the needs of multiple operators. They can select the appropriate OSS software based on their requirements and integrate it into their infrastructure.

System integrators and managed services

Telecom operators may opt for managed services offered by OSS vendors or system integrators. In this model, the vendor takes responsibility for deploying, managing, and maintaining the OSS solutions on behalf of the telco. This relieves the telco from the burden of handling the underlying infrastructure and allows them to focus on their core business

[19] https://telecoms.com/520012/global-ran-market-continues-to-stagnate/

activities. Managed services can include activities like software installation, upgrades, customization, and ongoing support.

In-house development

When economies of scale can be done, some telecom operators may have their own in-house teams dedicated to developing and maintaining OSS solutions. These teams work on creating customized solutions tailored to the specific needs of the telco. They leverage their expertise to build software and systems that address network management, service provisioning, performance monitoring, and other operational aspects.

Network management solutions follow a similar model to the one described for OSS. They are usually provided by equipment vendors, paired with their equipment.

3.3.3 Business support

As for network operations, depending on strategic choices and other factors such as legacy equipment dependencies and vendor dependencies, some operators develop their own in-house BSS solutions. This choice enables customization, bespoke functionality, and integration in existing systems, but requires substantial investments in terms of development resources, expertise, and ongoing support. Thus many operators choose a combined approach with some in-house developed components and outsourcing.

BSS solution providers. These are companies that specialize in developing and providing BSS software solutions to telecom operators, offering Commercial Off-The Shelf (COTS) solutions. They offer comprehensive systems that encompass various functions such as billing and revenue management, customer relationship management (CRM), order management, provisioning, mediation, rating, and charging.

System Integrators and managed services providers. System integrators are companies that assist telecom operators in implementing and integrating BSS solutions into their existing systems. Like for OSS, they ensure smooth integration with other operational and business support systems. Managed Services providers offer managed BSS services to telecom operators. They take care of the operation, maintenance (technical support, system upgrades, bug fixes, and system enhancements), and management of the BSS systems on behalf of the operators, ensuring smooth operations and high system availability. This category includes consultancy firms specializing in telecom BSS, that offer advisory and consulting services to operators. They provide expertise in BSS strategy, process optimization, system selection, vendor evaluation, and implementation planning. They assist telecom operators in identifying their specific needs and aligning their BSS systems with business goals.

Specialist BSS providers include:

- Billing and Revenue Management specialists. Some market players focus specifically on billing and revenue management services for telcos. They provide solutions and expertise to handle complex rating and charging models, billing accuracy, revenue assurance, and revenue optimization.

- Customer Experience Management (CEM) providers. CEM providers offer solutions and services to enhance the customer experience for telecom operators. They focus on areas such as customer self-service portals, personalized offers and promotions, customer analytics, and campaign management to improve customer satisfaction and loyalty.

- Data Analytics and Business Intelligence providers. These players offer advanced analytics and business intelligence solutions to telecom operators. They help operators leverage their BSS data to gain insights into customer behaviour, product performance, revenue trends, and market dynamics, enabling informed decision-making and targeted business strategies.

These categories of market players may overlap or collaborate with each other to provide end-to-end BSS solutions and services to telecom operators. BSS solutions providers may also be system integrators and Managed Services providers (e.g. Comarch, Ericsson, FTS, Huawei, IBM, Infovista, Mavenir, Netcracker, Nokia). Some stakeholders specialise in some services: billing and/or CRM for instance. Additionally, the BSS market is dynamic and continually evolving, with new players and service offerings emerging to meet the changing needs of businesses.

4. Key virtualization and cloudification concepts

Even for insiders, it is not easy to have a clear picture of what the various terms mean. This is partly because firms do not describe their propositions using standardised or consistent terminology. It is therefore essential to give a good definition for each term and the status of implementation. These definitions and descriptions of the concepts are set out below.

4.1 Virtualization

Virtualization is described by IBM as: *"Virtualization uses software to create an abstraction layer over computer hardware that allows the hardware elements of a single computer—processors, memory, storage and more—to be divided into multiple virtual computers, commonly called virtual machines (VMs). Each VM runs its own operating system (OS) and behaves like an independent computer, even though it is running on just a portion of the actual underlying computer hardware."*[20]*.* The benefits of this are that resources are shared and can be added and removed according to the needs of the users. A hypervisor (a software that creates and runs virtual machines) coordinates resources between the different virtual machines, so that they are available to all virtual machines and do not interfere with each other.

Virtualization is not limited to servers, but can work for all kinds of infrastructure elements, such as storage, CPU, GPU, application, network and data centre. Data centre virtualization is often referred to as infrastructure as a service (IaaS). Data centre virtualization abstracts most of a data centre's hardware into software, effectively enabling an administrator to divide a single physical data centre into multiple virtual data centres for different clients. For this report, network virtualization is particularly important, because it underlies software defined networking (SDN), Network Function Virtualization (NFV) and OpenRAN.

Containerisation must be distinguished from virtualization. Virtualization abstracts the underlying hardware away from the operating systems that run on it. Virtualization allows multiple operating systems to run applications on the hardware. This leads to some inefficiency as each virtual machine requires resources for the operating system in addition to resources for the application. Virtual machines are more physically constrained and dependent upon the underlying hardware and have to be adapted for different hardware (i.e. in a different data centre). Containerisation removes the dependence upon the virtual machine and underlying hardware. Containerisation allows multiple applications to run independently in a container engine. As long as the container engine functions the same, it can be started on any platform anywhere. In virtualised environments a container makes it even easier to activate applications and this can be done on different infrastructures in different locations.

[20] What is virtualization?, source: IBM https://www.ibm.com/topics/virtualization

The container doesn't make assumptions on the underlying hardware and virtual machine and should therefore be able to operate anywhere.

The various ways that virtualization and containerisation abstract the physical resources away from the underlying hardware and the applications running over them allows infrastructure, platforms and software to become services. Customers don't have to buy hardware, operating systems and applications, but instead can rent them according to their needs. This creates financial trade-offs between CAPEX and OPEX, and the degree of control network operators have over performance and functionality. In addition, new generations of hardware enable new functions to become virtual and even to be moved to a container. This allows generic hardware to perform functions that used to require specialised hardware and, vice versa, allows specialised hardware to become available to more applications and processes.

4.2 Software Defined Networking (SDN)

Software defined networking is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure to direct traffic on a network[21]. This means that the forwarding process governing how data is directed to the next location is separated from the routing that determines what route the traffic takes through the network. Such functionalities were present in earlier networks too, for example in telephony networks where a controller software would route calls over links and redirect them if a particular route became unavailable.

Virtual networks were to some extent a SDN predecessor too. A VLAN in ethernet or similar types in other protocols, allows a physical network to be segmented into different logical networks. This way in an office environment access to the server that handles the payments, would only be accessible to the authorised people and computers in the payments department. The same computers/staff could be a member of different virtual networks, so that they would be able to reach shared printers, file servers and other shared resources. SDN extended this concept further by centralising the management of traffic flows.

SDN received increasing attention in the early 2000s when the scale in both data centres and wide area networking across the globe would run into scalability issues. The IETF worked on OpenFlow which is widely implemented to support SDN. OpenFlow enables network controllers to determine the path of network packets across a network of switches. The controllers are distinct from the switches. This separation of the control from the forwarding allows for more sophisticated traffic management than is feasible using access control lists (ACLs) and routing protocols.[22] Separating control over routing from forwarding was initially considered risky because it requires a very reliable connection between the control function

[21] https://www.vmware.com/topics/glossary/content/software-defined-networking.html

[22] https://en.wikipedia.org/wiki/OpenFlow

and the forwarding function. When the reliability of the networks was improved, the operators increasingly saw uses for SDN in operating networks.

In a traditional network topology a router is considered “full” when it hits 40% of its peak capacity[23]. This is because the dynamics of data flows can be such that the traffic is all to or from a small number of links that are saturated as a result. It is difficult to get beyond that number because unexpected events can create traffic spikes. In a large-scale network, where the user demands are stable and unexpected peaks can be dealt with dynamically, the network can be scaled and managed, so that use reaches the theoretical 100% utilisation. This saves significant investment in the network; it also allows more flexibility in how to direct traffic flows and increase the reliability of the network.

The way SDN delivers efficiency, scalability, control, reliability and saves money is different within the datacentre than outside the datacentre.

- Within the datacentre, the controller will know what types of applications are functioning, what the service level requirements are and what jobs are scheduled. The scheduler then has to optimise the distribution of resources and tasks, across all applications and demands within the service requirements that have been set. Within a datacentre the complexity is focused on making sure every part of the computing equipment can operate to the fullest capacity possible, without over- and under-provisioning.
- Outside the datacentre, in a Wide Area Network (WAN) the role of an SDN is aimed at making use of all available capacity, while dealing with planned and unplanned outages. SDN allows those that operate the network to define the parameters for each link and policies for fail-over, i.e., if and when an element fails, the system can switch to another one. Though this sounds basic, the reality is significantly more complex. In another project on resilience of submarine networks several respondents stated[24] that, when planned or unplanned events happen, SDN helps with controlling how data flows are handled in the network. Either the customer is directed to another datacentre, or the response to the end-user comes from a different location than usually expected. In telecom WAN such techniques are primarily deployed to deliver the most optimal routing experience for all those who use the network, despite planned and unplanned events.

The initial fears about separating the control functionality from the forwarding functionality not being robust enough, have been alleviated in OpenFlow and similar implementations. However, the concerns remain valid because for SDN to work at scale, it has to be able to deal with failures at scale as well. This will be referenced in the section on cloudification.

[23] See for example Modern Cloud Networking: Delivering Network Services at Scale using Andromeda (Cloud Next '18), Babi Seal, https://youtu.be/9CbcIfZ3zH4. To explain SDN and cloudification some examples from Google are used to make the reader gain some understanding of how SDN and cloudification function at scale. The reason Google was used is because it gave some accessible explanations on the topic. Other large-scale cloud and CDN operators dealt with similar issues and used similar solutions.

[24] https://www.stratix.nl/vier-vragen-aan-rudolf-over-zeekabels/

4.3 Network Function Virtualization (NFV)

In its simplest form, a digital telecommunications network allows various endpoints to connect with each other and exchange data. The network therefore needs to send and receive data. The simplest networks broadcast to all. To improve efficiency on the use of available resources, all kinds of functionality is added to networks. For example, addressing to make point to point connections possible, interconnection so that other networks can be connected or authentication and authorisation to check whether the devices are who they say they are and are allowed to do what they want to do. The number of functions quickly adds up; load balancers, intrusion detection, firewalls, routing tables, session controllers, border gateway protocol, provisioning and configuration etc. All are needed to make a large-scale network function, whether it is in a data centre, in a single telecom network or a global network for a specific firm or service. These functionalities used to be either combined and integrated into a router or switch or to have specific hardware, for example a firewall.

Network Function Virtualization allows all the various network functions to be virtualised so that they can be shared across the physical network by the specific services and applications running over them. It also allows one physical network to function as multiple different logical networks, or to combine networks of different infrastructure companies to function as one logical network. A virtualised function can then provide these services across the network, without physical hardware needing to be present everywhere. It can make the network more resilient, because instead of relying on a number of pieces of hardware, the function can be spread over multiple servers across the network either in a virtual machine or in a container.

NFV is different from SDN. SDN focuses on how traffic flows through the network, where it separates the equipment that receives, directs and transmits the data, from the part that controls that process. NFV virtualises the functions that determine what is done with the traffic in the network.

4.4 Cloudification

Cloudification can be seen as an extended form of datacentre virtualization. Instead of a virtual computer running on one server, the applications are abstracted away from the hardware. Cloudification was enabled by the developments in virtualization that preceded it, it and developed the concept further and at greater scale. The scale of these new systems and their huge requirements for data storage made it hard for existing hardware to cope, creating challenges for large scale cloudification. It has been necessary to overcome these challenges to create efficient and cost-effective hyperscale cloud solutions.

Virtualization and containerisation as described in the previous paragraphs was to some extent limited to the hardware. For example disk-drive standards such as Small Computer System Interface (SCSI) standards defined how many drives could be connected in a redundant array of disks. The disks and arrays were high quality and had many fail safes, which meant they were expensive. The data on it was extremely valuable to the firms, so the costs were proportionate in the eyes of the firms that bought them. The limits on the number of disks and other parameters were so high that they did not pose serious issues for the large firms using them at that moment.

When cloudification started, the internet firms initially made use of this high-quality hardware intended for large corporations. They then quickly encountered the limits because their scale was significantly larger than even the largest multinationals and governments when it came to number of processors, disks, networks and other resources. The consequences of this were explained at the North American Network Operators Group, an informal meeting of those who operate internet networks. In 2010 a keynote by Google's senior architects had the title: "Worse is Better"[25]. Even then, a single storage cluster contained 2400 servers with 4.8 petabyte storage, 30 terabyte of memory and there were warehouses full of such clusters. They explained that as a result they had to factor in that no matter how reliable the manufacturer would guarantee there were so many components (memory, power supplies, disks, switch ports, routers etc.), failures were inevitable. This was in addition to other possible problems, such as severe weather events. For the cloud, the high reliability hardware could not handle the required scale and so did not provide an economic advantage over commodity hardware.

To make cloudification work, the lessons of SDN and NFV had to be applied at scale to make sure that services would continue to be provided, despite unexpected problems in hardware and fluctuating use. Providers started to differentiate between two classes of traffic: user traffic to and from the user; and cloud-internal traffic.

These two classes of traffic have different requirements in service level and quality, and different scale. Machine traffic is by far the largest proportion. This is in part because there is a need to protect against failure. One picture a user uploads to backup needs to be copied multiple times and stored in different locations for safe keeping. Dealing with failure will initiate new data flows just to meet minimum reliability requirements. In addition, cloud providers offer their customers compute power to process data, which increases data traffic flows.

A benefit mentioned by Google was that SDN allowed it to shift tasks from one generation of datacentre to another when new equipment became active, hence also freeing capacity to re-use the old datacentre for other tasks. This contributes to higher utilisation of the available capacity in networks.

Issues related to separating the control function from the forwarding function emerged. As the network scaled and incorporated tens of thousands of switches, the control plane faced scaling issues, because of hardware and network failures. Updates to the control plane and the underlying forwarding plane would become too frequent and themselves create a bottleneck

[25] « Worse Is Better » Vijay Gill/Bikash Koley/Paul Schultz for Google Network, Architecture, Google, June 14, 2010, NANOG 49, San Francisco

for scaling. To deal with this, a hierarchical control plane was introduced that allowed further scaling.[26]

The consequence of this is that the way SDN and NFV scale in cloud computing is different in two ways from how it works in a single (telecom) company or datacentre environment:

1. Towards the user, it focuses on delivering the service within the Service Level Agreements (SLA). Regardless of the state of the networks both outside the control of the cloud provider and the networks operated by the cloud provider, it has to work within the parameters. This means that a cloud provider has to be able to shift workloads across geographies and not lose data or functionality. Telecom firms in particular are limited to the geographic locations where they operate.

2. Within the cloud, there is a constant drive for efficiency and scale. This means that everything is used all the time, while also handling the addition of new equipment and datacentres, failures and unexpected events. This is a different challenge to managing a telecoms network where the network is stable, average usage is relatively low, but short peaks have to be handled.

In many ways, a hyperscale datacentre is significantly different from more traditional computing particularly within telecom firms. The difference is important to consider, when the effects of the various developments in virtualization, software defined networking and cloudification are evaluated. It also means that not all developments in cloudification are directly transferable to other firms and in particular telecom firms.

4.1.1. The impact of cloudification for telecom firms

The impact of cloudification in telecom firms is different to global hyperscale cloud infrastructure providers because telecom firms are restricted by geography. They provide access networks in a particular area. This means that the part of the telecommunications firm that supports this doesn’t benefit from cloudification as much as the part that handles functions which are not tied to the geographical area, such as BSS.

Within telecom firms, BSS is sometimes shared between different operating entities in different countries. In other cases there is a vendor who provides the applications as a service to various operators around the globe. Cloudification allows some of these systems to be scaled more efficiently, for example scaling up for the end of the month billing cycle and scaling down when it has been completed. It is beneficial to have systems that are not tied to a particular

[26] Chi-Yao Hong, Subhasree Mandal, Mohammad Al-Fares, Min Zhu, Richard Alimi, Kondapa Naidu B., Chandan Bhagat, Sourabh Jain, Jay Kaimal, Shiyu Liang, Kirill Mendelev, Steve Padgett, Faro Rabe, Saikat Ray, Malveeka Tewari, Matt Tierney, Monika Zahn, Jonathan Zolla, Joon Ong, and Amin Vahdat. 2018. B4 and after: managing hierarchy, partitioning, and asymmetry for availability and scale in google's software-defined WAN. In Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication (SIGCOMM '18). Association for Computing Machinery, New York, NY, USA, 74–87. https://doi.org/10.1145/3230543.3230545

location, data centre or geography, because it adds flexibility, redundancy, scale and efficiency.

For the network support systems cloudification is also less relevant because the geographic location of a network and its customers. It isn't possible to move the provision of fixed and mobile internet from one town to another. For example, the control of base stations in 5G requires a controller with up to 30km of fibre length. This means that the network resources at each location have to be adequate for peak demand, whether it is daily, seasonal, unexpected, and operators factor in future demand as well. A telecom network therefore has to have a significant level of local unused resources to deal with different situations that might arise. To summarise, a well-run network almost never reaches the peak of its capacity, whereas a well-run cloud system almost always runs at peak capacity.

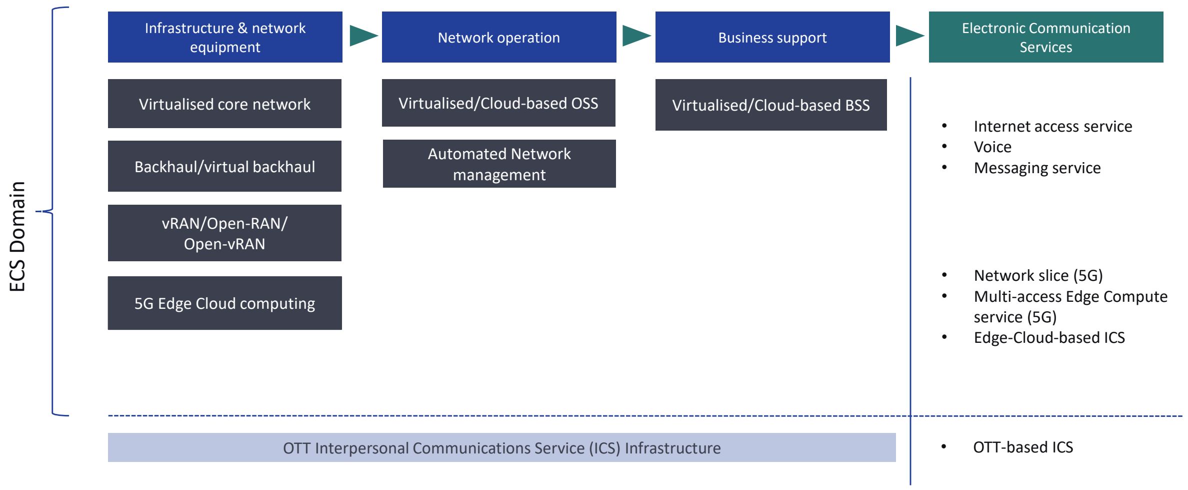
The effects of cloudification are more pronounced in mobile networks than fixed, because mobile networks are more uniform on a global scale. Fixed networks tend to be different in each market, and the way each operates is determined by local market conditions and regulations. This is different from mobile networks where there are many multinational mobile network operators. In addition, the networks and services for mobile networks are manufactured and provided by a smaller number of vendors, such as Nokia, Ericsson, and Huawei on a global scale and in a uniform fashion. The result is that cloud-based business support has more scale benefits for mobile networks. This is even true in the way local mobile networks operate, because even though the systems may have to be placed locally they still function in the same way as elsewhere, which makes it possible to create standardised ways to operate and interact with local parts of mobile networks.

5. The evolved ECN/S model

5.1 Components of the evolved ECN/S value chain

In this section, we describe how the traditional model for mobile ECN/S value chain is being transformed. As more MNOs virtualise, softwarise and cloudify their network, the transformation is expected to give rise to a new set of components in each of the three building blocks of the value chain as shown in Figure 5.1.

Figure 5.1: Components of the evolved mobile ECN/S value chain


ECS Domain
Infrastructure & network equipment
Network operation
Business support
Electronic Communication Services
Virtualised core network
Backhaul/virtual backhaul
vRAN/Open-RAN/ Open-vRAN
5G Edge Cloud computing
Virtualised/Cloud-based OSS
Automated Network management
Virtualised/Cloud-based BSS
Internet access service
Voice
Messaging service
Network slice (5G)
Multi-access Edge Compute service (5G)
Edge-Cloud-based ICS
OTT Interpersonal Communications Service (ICS) Infrastructure
OTT-based ICS

5.1.1 Infrastructure and network equipment

Core network transformation

There has been widespread use of NFV to transform the core network of MNOs. The transformation of an Evolved Packet Core (EPC) of an LTE network involves virtualization of network functions that provide network services in the key components of the EPC. These components include Mobility Management Entity (MME), Serving Gateway (SGW), Packet Data Node Gateway (PGW) and Policy and Charging Rules Function (PCRF). Cloud infrastructures are being used to host virtual machines that execute the network functions for these components' services. This has the effect of moving the network into the cloud.

The possibility of cost savings through the use of generic hardware with virtualised network functions (VNF) as well as the deployment of cloud-native 5G mean that MNOs have been turning to cloud infrastructures for the past 6-7 years. First, physical cloud infrastructure – including computing hardware, storage devices and networking equipment – and abstracted resources (software), which enable the system to use the physical resources in the hardware,

are deployed across an MNO's core network. Abstracted resources provide virtual memory, computing power and storage.

An NFV infrastructure (NFVI) platform is then implemented on the cloud infrastructure to enable VNFs for core network to be hosted and managed in the cloud. An NFVI platform typically comprises an operating system, hypervisor, a Virtual Infrastructure Manager (VIM) and NFV Orchestrator. The network services constructed through different VNFs can then be managed and delivered to different nodes as and when needed through the NFVI platform. An NFVI platform implemented in a cloud infrastructure is more commonly known as a Telco Cloud Infrastructure.

Often multi-vendor VNFs can be deployed on a Telco Cloud Infrastructure, which also has the capability to manage and orchestrate these VNFs and the underlying infrastructure. The most ubiquitous Telco Cloud Infrastructures, such as VMware's Telco Cloud Infrastructure, are SDN-based.

An alternative to the deployment of a private cloud infrastructure is the use of a public cloud or a virtual private cloud running on a public cloud. An MNO may choose to host its 5G core and IMS functions on a public cloud, such as AWS Regions or Microsoft Azure, which can also be managed by the public cloud provider. There would then be a backhaul connection between the MNO's edge cloud network hosting the CU (Centralised Unit) and the public cloud where the core network is hosted.

In summary, the virtualization, softwarization and cloudification of core network, which leads to centralisation of network functions in the cloud, splits it into 3 broad sub-components namely: VNFs, NFVI platform and Cloud Infrastructure.

Backhaul transformation

Mobile backhaul is the transport network that connects the core network and the RAN (Radio Access Network) of the mobile network. As such, its sole function is the transport of voice and data traffic to and from the RAN and the core network over a physical transport network. The absence of true network functions, other than routing and some types of switching, in this physical transport network makes virtualization techniques such as NFV less relevant for backhaul.

Virtualization of backhaul has been examined in academic contexts to provide solutions to specific problems. For example, Ginnan et al. propose a regime of dynamically assigning bandwidth to each service in a virtualised backhaul of a virtualised access area of a WLAN network that is used to supplement a public mobile network. The aim is to reduce the call-blocking probability of users with a guaranteed bit rate while improving the service satisfaction of users served on a best-effort service.[27] Li et al. propose a model for establishing a market for virtual backhaul that can be used by virtual operators to examine the implications for green energy use in mobile backhaul networks.[28] However, they do not represent solutions that rely on NFV.

While there are few commercial solutions that involve NFV, the use of software-defined networking principles for backhaul appears to be gaining traction. This is due to the expected increase in adoption of network fabric architecture for 5G backhaul networks.

A network fabric is a type of network topology where all nodes, including switches and endpoints, are interconnected to all other nodes. This type of network topology can help to optimise performance by allowing latency-sensitive 5G applications to be located in aggregation nodes near the network edge instead. These 5G applications would otherwise have to be accommodated in the far edge of the network to achieve the required latency. An SDN controller can then be used to manage a network fabric to set up the relevant overlay networks to route traffic optimally. Both Nokia and Cisco offer such backhaul solutions.

Even though NFV does not directly affect backhaul connections that are self-supplied or purchased on a wholesale basis from other telecom operators, moving the core network into a public cloud has made it possible for a new type of backhaul service to enter the market. A public cloud provider can offer its own optical network service to connect an MNO's RAN edge to the public cloud, where the MNO's core network resides. Therefore, virtualization, softwarization and cloudification of the core network could be said to indirectly give rise to virtual backhaul.

RAN transformation

The process of virtualization and softwarization of RAN is best illustrated through the transition of legacy RAN to Open RAN. In 3G and early 4G networks, RAN was deployed with co-located radios (remote radio head – RRH, remote radio unit – RRU) and baseband units (BBU) as previously mentioned. BBUs are connected to the mobile core through the backhaul network. This type of deployment is called distributed RAN (D-RAN), which was implemented with proprietary-based equipment from the likes of Ericsson, Huawei and Nokia.

Virtualised RAN (vRAN) is a type of deployment, which is based on NFV principles. In effect, proprietary RAN systems are virtualised into software that run on Commercial-Off-The-Shelf (COTS) hardware, such as servers with Intel or ARM-based CPU's. The advantage of vRAN

[27] Kazuhiko KINOSHITA, Kazuki GINNAN, Keita KAWANO, Hiroki NAKAYAMA, Tsunemasa HAYASHI, Takashi WATANABE, "Public WLAN Virtualization for Multiple Services", IEICE Transactions on Communications, vol.E102.B, no.4, pp.832, 2019.

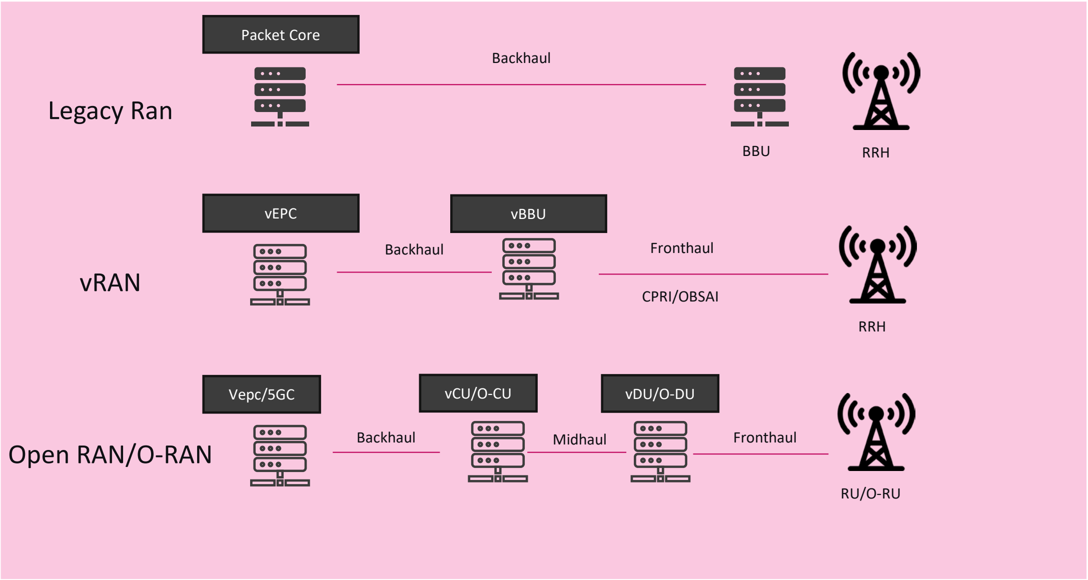
[28] D. Li, L. Gao, X. Sun, F. Hou and S. Gong, "A Cellular Backhaul Virtualization Market Design for Green Small-Cell Networks," in IEEE Transactions on Green Communications and Networking, vol. 3, no. 2, pp. 468-482, June 2019, doi: 10.1109/TGCN.2019.2904975.

is that it increases flexibility and can help to reduce the cost of RAN through the use of commodity hardware.

Open RAN is a term used for an architecture which has the following characteristics:

- The RAN has disaggregated components;
- The interfaces between these disaggregated components in the RAN need to comply with standards that have been agreed and openly defined, making the components interchangeable between vendors; and
- The functional splits of the work carried out by the components have to be determined in a specific implementation such that the splits conform to the options defined by the 3GPP (split options 1 to 8).

Figure 5.2: From legacy RAN to Open RAN



Source: AvidThink, Plum Analysis

In the Open RAN (including Open RAN based on O-RAN specifications) above, the vBBU (RRH+BBU) is now separated into a centralised unit (CU), a distributed unit (DU) and a radio unit (RU). The fronthaul connects DU to the RU, the mid-haul link connects the DU to the CU, while the CU is connected via a backhaul to the mobile core. CU, DU and RU do not have to reside in different geographic locations. A single CU can serve multiple DUs, just as a DU can be attached to multiple RUs.

Open RAN has been designed with cloud-native virtualization principles and technologies to address the lack of network equipment's interoperability. However, an Open RAN's deployment can also use physical components. Interoperability would enable network engineers to combine units from different vendors.

Components used in an Open RAN deployment (including hardware, software, both cloud and virtual) may not always be completely compatible due to their multivendor nature. To optimise the performance and strike a balance between two often incompatible components, Open RAN allows engineers to select which unit should be deployed to which operation. The network engineer can make use of functional split to place Virtual Network Functions (VNF) across different components along a single path. This functional split can also be applied to older generations of mobile technology, such as 2G, 3G, and 4G, despite being introduced in 5G NR.

As previously mentioned, not all radio network equipment needs to be fully virtualised in an Open RAN environment. Many radio units can still be the same physical components, which operate as specific standard hardware products. This means that the Open RAN concept is not the same as Open vRAN or vRAN even though there are overlaps between these concepts. Open vRAN and vRAN are based on virtualization, but while one is open, the other is not. Open RAN can be a partial vRAN or a full vRAN.

The virtualization, softwarization and cloudification of RAN splits it into 3 broad sub-components namely: radios, vRAN software solution and Cloud Infrastructure. Radios and RAN software and hardware were sold together in the traditional model as proprietary solutions by traditional network vendors such as Nokia, Ericsson and Huawei as previously mentioned.

RAN edge

In vRAN and Open RAN, the computing power is removed from the radios. The DU in an Open RAN can, in fact, serve multiple radio units at different physical locations. This makes it necessary to deploy servers and data centres closer to the sites of the radios. Data from users would otherwise have to travel into the core network to be processed, which would result in higher latency. RAN edge has, thus, become a crucial part of an MNO's RAN. This could be thought of as a de-centralising effect of virtualization.

RAN edge

The radio access network (RAN) edge is outside the network core and closer to the end user. RAN nodes at the edge (RAN edge) connect users to the core network, clouds, the internet more generally, and to other users without user data travelling as far before reaching the nearest RAN node. Adding general purpose servers to a RAN node gives the node more compute, networking, and storage resources to use. Types of RAN nodes can be traditional cell towers, rooftop antennas, or small cell deployments more common with 5G RANs. An alternative to installing servers at a node is using a local data centre to serve multiple nodes.

Another reason MNOs are actively deploying processing and storage capabilities at the RAN edge is the latency requirements of anticipated 5G applications. Applications that require ultra-low latency can only be provided if user data can be processed without delay, which would not be possible if the data has to traverse the core network. MNOs do not always need to install these facilities themselves, however. It is possible to purchase them as a service from cloud providers such as AWS. One example is AWS Local Zones, which can be used to host 5G RAN CU. Using such an edge solution can give the MNO a fully integrated solution if its core network is also hosted with the same cloud provider.

The possibility of bringing a public cloud's capabilities closer to the users through the RAN edge has also spurred partnerships between cloud providers and MNOs. In many markets, including the US and Europe, MNOs have started to launch Multi-access Edge Computing services (MEC) in collaboration with cloud providers. MEC services offer application developers and content providers cloud-computing capabilities and IT service environment at the edge of the mobile network.[29]

To provide MEC services, the cloud provider deploys an infrastructure that embeds its compute and storage services in the MNO's data centres at the RAN edge. This enables application traffic to reach application servers without leaving the MNO's network. This contrasts with the traditional model, where the traffic needs to traverse the MNO's core network and then to the Internet before reaching the cloud provider's application servers. AWS Wavelength, which is used by both Verizon in the US and Vodafone in Europe, is an example of such RAN edge infrastructure.[30]

Co-location of infrastructure at an MNO's RAN edge's data centres also enables cloud providers to offer enterprise-grade connectivity to the MNOs' business customers. The service could be virtualised in the edge cloud rather than offered over a native app on the customer's device. This increases flexibility for the user, as it could allow seamless handover across devices.

5.1.2 Network operations

Virtualization and cloudification have a significant impact on OSS, transforming the way networks are managed and operated. OSS systems now need to handle the provisioning, deployment, scaling, and management of virtualized network functions and play a crucial role in orchestrating SDN controllers, managing network policies, and ensuring efficient utilization of network resources.

In addition, cloud computing has enabled the emergence of cloud-based OSS solutions. Instead of maintaining complex on-premises infrastructure, operators can deploy OSS systems in the cloud, benefiting from scalability, elasticity, and cost-efficiency. Cloud-based

[29] https://www.etsi.org/technologies/multi-access-edge-computing
[30] https://aws.amazon.com/wavelength/faqs/

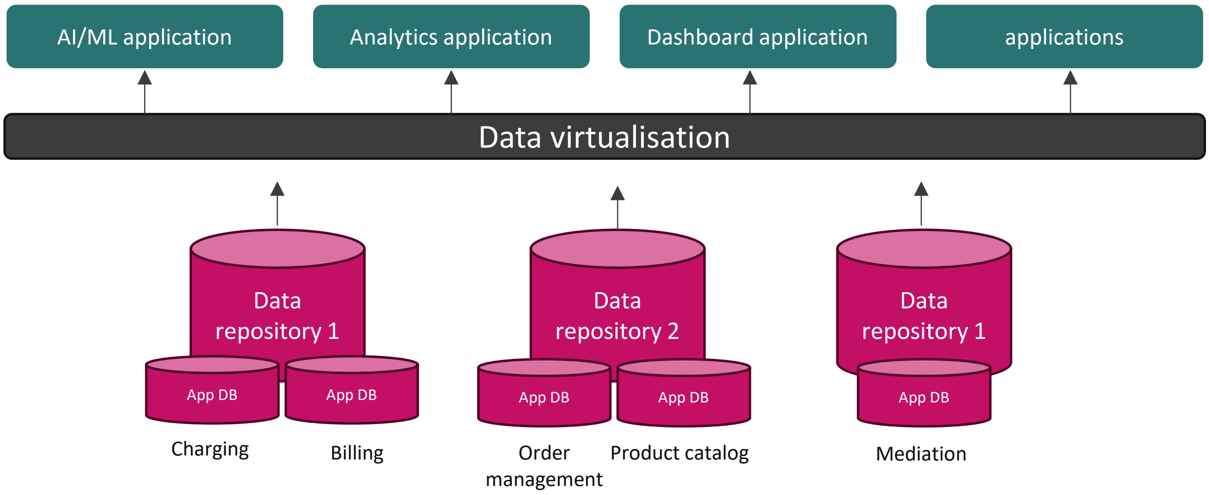
OSS solutions offer easy accessibility, rapid deployment, and the ability to scale resources based on demand. With cloud computing, software is hosted on the servers of a third-party service provider. In this setup, there are little to no management needs as the provider will handle maintenance and security.

Regarding the network management component, instead of managing physical network devices, network managers now must handle virtualized resources, virtual machines (VMs), containers, and software-defined networking (SDN) controllers. This complexity requires a shift in network management practices and the adoption of new tools and processes to effectively monitor, configure, and troubleshoot virtualized environments.

5.1.3 Business support

As mentioned in Section 3.2.3, data in traditional BSS is spread out in different data systems repositories[31]. Through a layer between data sources and data consumers, data virtualization has enabled integration of data silos (Figure 5.3). It contains only the metadata required to access the sources (data remains in the source). It provides logical views of business entities without making physical copies of data and combines a variety of data repositories. It is location agnostic, meaning that data can come from the premises or from cloud. Data virtualization is useful for applications like analytics and AI/ML as they need cumulative and holistic data - not only individual records.

Figure 5.2: Data virtualization integrating multiple BSS data repositories



Source: Ericsson[32]

[31] A repository holds data from various sources either in their native format (in which case it is called a data lake) or in transformed format (in which case it is called a data warehouse).
[32] https://www.ericsson.com/en/blog/2022/1/data-virtualization-integrate-bss-data-slios

BSS virtualization enables telecom operators to have a consistent data governance, to optimize costs and improve productivity via an easier, faster, unified and secured access to data thanks to minimized data replication.

When data is located in the cloud – and not in premises, this is called cloud-based BSS. Compared to traditional on-site BSS, telecom operators can benefit from:

- a quicker BSS deployment (chip and hardware shortages can delay on-site deployment by 3-6 months, whereas cloud BSS can be ready for service in 30 days),
- scalability (cloud-based BSS helps scale a business with relatively lower investments, letting operators introduce new capabilities and modules without making costly changes to their core systems,
- costs savings, and
- a better customized customer experience through an improved customer retention and loyalty, hence potential increased revenues.

5.1.4 OTT-based ICS

Some Interpersonal Communications Services (ICS) are delivered over the Internet (such services have often been referred to as “over-the-top” – OTT). Delivery of these services is largely unaffected from a technical point of view by the evolution of ECN functions through cloudification, softwarization and virtualization described in this report. Where these services rely on ECNs for delivery of data (for example over a RAN), this is captured by our analysis of ECN changes.

In the evolved model compared to the traditional one, lines between roles in the value chain and the categories of services are blurring, with some OTT ICS becoming more integrated to the telecom value chain. An example is mobile network operators integrating mobile voice services with Microsoft Teams for large business customers.[33] Telephony with E.164 numbers is then handled in the same way as videocalls using Microsoft Teams. Where traditionally there were strict separations between number dependent and number-independent communication services, this is an example where the lines are blurred, and what used to be separate is now one service. To enable this, there is coordination between the voice operator and the over-the-top provider, which in this case is Microsoft.

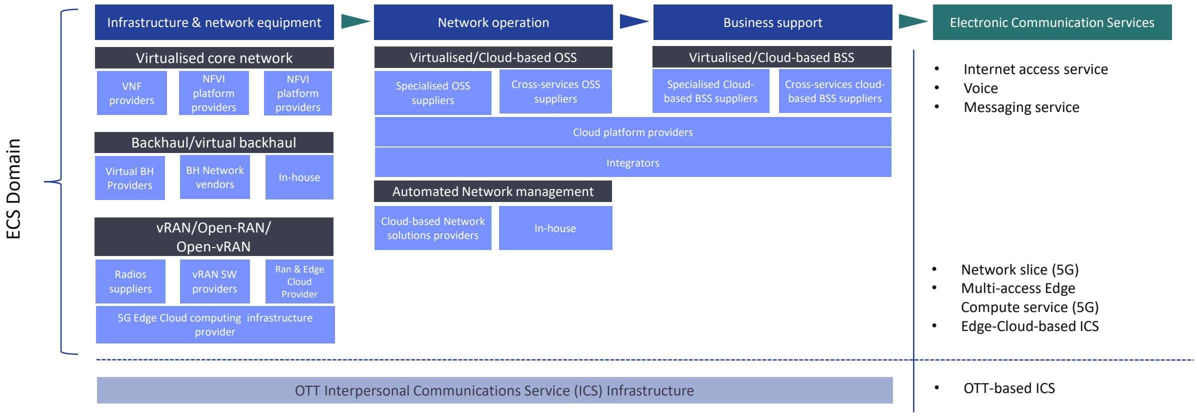
5.2 Markets for supply of components/services in the evolved model

New players have entered the market and specialized in specific areas of the value chain. New business models have emerged and the relationship between the different players has

[33] See Microsoft Connect https://learn.microsoft.com/en-us/microsoftteams/operator-connect-plan

become increasingly dynamic. The transformation of the mobile ECN/S value chain, elaborated in the previous section, is leading to a corresponding transformation of the markets for the supply of each component of the value chain. The key groups of players involved in the supply of each component are shown in Figure 5.3.

Figure 5.3: Suppliers of the evolved mobile ECN/S value chain



ECS Domain
Infrastructure & network equipment
Network operation
Business support
Electronic Communication Services
Virtualised core network
VNF providers
NFVI platform providers
NFVI platform providers
Backhaul/virtual backhaul
Virtual BH Providers
BH Network vendors
In-house
vRAN/Open-RAN/ Open-vRAN
Radios suppliers
vRAN SW providers
Ran & Edge Cloud Provider
5G Edge Cloud computing infrastructure provider
Virtualised/Cloud-based OSS
Specialised OSS suppliers
Cross-services OSS suppliers
Virtualised/Cloud-based BSS
Specialised Cloud-based BSS suppliers
Cross-services cloud-based BSS suppliers
Cloud platform providers
Integrators
Automated Network management
Cloud-based Network solutions providers
In-house
• Internet access service
• Voice
• Messaging service
• Network slice (5G)
• Multi-access Edge Compute service (5G)
• Edge-Cloud-based ICS
OTT Interpersonal Communications Service (ICS) Infrastructure
• OTT-based ICS

Note: The term Vendors refer to manufacturers and sellers of network equipment, suppliers are firms that that supply solutions that may comprise both hardware and software, and providers denote firms that primarily provide software or data-based service or managed software/data-based service through their own physical infrastructure.

We explain in this section how the markets for the supply of the value chain components are changing as shown above. Market trends are also discussed in following sections.

5.2.1 Quantitative market data

Reliable quantitative data on the market is difficult to find. Much available data is the result of subjective analysis and there are a broad range of forecasts. However, it is reasonable to assume that the migration of network functions, operations and business support to cloud environments is tangible, and expected to grow.

Global telco cloud

Available forecasts include:

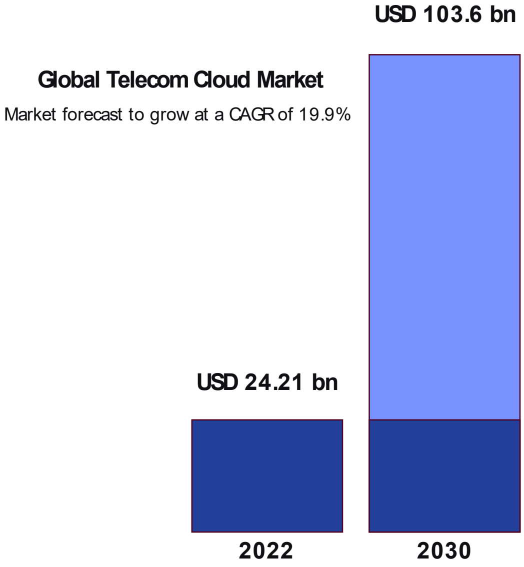
- Cap Gemini forecasts that 31% of global network capacity is being serviced by cloud today, and this is expected to increase to 46% in the next 3 to 5 years.[34]

[34] https://www.capgemini.com/insights/research-library/cloudification-of-networks/

- Cap Gemini survey data indicate that, by transforming to cloud, telcos can improve their network total cost of ownership by $260 to $380 million and can gain an early-mover advantage to the tune of $110 to $210 million in additional revenue. [35]

- The global telecom cloud market size is expected to reach USD 103.6 billion by 2030, according to this report. The market is anticipated to expand at a CAGR of 19.9% from 2022 to 2030.[36]

Figure 5.4: Growth forecast for the global telecom cloud market



- In 2021, North America emerged as the largest market for the global telecom cloud market, with a market share of around 35.5% and 19.7 billion of the market revenue. The Asia-Pacific market is expected to grow at the fastest CAGR between 2021 and 2030[37].

Open RAN

- Global Open Ran market is anticipated to increase from USD 1.1 billion in 2022 to USD 15.6 billion by 2027, At a CAGR of 70.5% over the period.[38]

- In December 2021, the UK Department of Culture, Media and Sport (DCMS) announced that it has agreed with the four domestic operators to fulfil a goal to boost deployments

[35] https://www.capgemini.com/insights/research-library/cloudification-of-networks/

[36] https://www.researchandmarkets.com/reports/5649342/telecom-cloud-market-size-share-and-trends?gclid=CjwKCAjwqZSlBhBwEiwAfoZUIHggh02YGb3kKzqzWCcylSkFMd6GW8BTnPW2qd9VQQkzvdxmb-8WKxoCQbwQAvD_BwE

[37] https://www.sphericalinsights.com/reports/telecom-cloud-market

[38] https://www.marketsandmarkets.com/Market-Reports/open-ran-market-153445936.html?gclid=CjwKCAjwqZSlBhBwEiwAfoZUICqREanGnu7o8ONMKfTW5CpQzJ--eATw4fLdqMcJEQKKEnkMhLnpgxoC_YwQAvD_BwE

setting a target of 35% of the nation's mobile network traffic is carried over open RAN by 2030[39].

OSS/BSS

- According to recent Omdia's Telecom[40] Cloud Evolution Survey, approximately 4% of telco IT (OSS and BSS) workloads are hosted on the public cloud currently (mainly BSS) and respondents expect this to rise to 23% in 5 years.[41]

- In its Cloud OSS BSS Market analysis report[42], Future Market Insights – a market research company- indicates that in 2021, cloud OSS BSS global market was about US$ 24 billion. The market growth over the next 10 years is projected to be at 8.4% CAGR reaching a valuation of 60 billion by 2032.

5.2.2 Infrastructure and network equipment

Core network

As explained in Section 5.1.1, the virtualization, softwarization and cloudification of core network has led to the splitting of core network into three broad subcomponents, namely:

- The cloud infrastructure;

- The Telco Cloud Infrastructure platform; and

- The Virtualised Network Functions.

The cloud infrastructure encompasses the totality of physical and abstracted resources of a cloud network, as well as the software interface for making use of all available resources in the cloud network. The Telco Cloud Infrastructure platform sits on top of the cloud infrastructure and enables core network's VNFs to be developed, deployed and managed. The platform also has a controller for network resources inside and outside the platform that provides connectivity between VNFs and PNFs. This controller is typically based on SDN principles.

[39] https://www.globenewswire.com/en/news-release/2022/03/08/2398558/28124/en/Global-OPEN-RAN-Market-Outlook-An-Opportunity-worth-32-Billion-by-2030.html

[40] In July 2022, Omdia surveyed 49 senior operations and IT decision makers among telecom operator.

[41] https://www.thefastmode.com/expert-opinion/28079-what-will-2023-look-like-for-telecoms

[42] https://www.futuremarketinsights.com/reports/cloud-oss-bss-market#:~:text=What%20is%20the%20sales%20forecast,8.4%25%20from%202022%20to%202032.

Virtualised Network Functions for core network can then be deployed on the Telco Cloud Infrastructure. VNFs are made available to the MNOs for purchase through an online platform by the NFVI platform provider. For example, VMware offers VNFs through its marketplace, which are developed by multiple companies. These include traditional telecommunications equipment vendors, such as Nokia and Ericsson, through to software developers, such as GitLab and Cloud Vector.

The disaggregation of the core network equipment into the three subcomponents has effectively created new markets in the supply of core network solutions. Different types of core network equipment were sold by integrated network vendors, such as Nokia, Ericsson and Huawei, in the traditional model. In the evolved model, there is a market for cloud infrastructure, a market for Telco Cloud Infrastructure platform, and a separate market for VNFs.

Backhaul

The limited role of NFV in backhaul network transformation means that there is no need for Telco Cloud platform. Physical mobile backhaul continues to require a suite of different transport solutions, including microwave and optical (including xPON) technologies. The implication is that the systems that are self-provided by the MNOs will continue to be supplied by backhaul equipment vendors and suppliers of physical data links – i.e. telecom operators.

However, the use of virtual backhaul by MNOs to connect their RAN edge with their core network in a public cloud could usher in new players. Products like AWS Direct Connect are being used by DISH to backhaul data traffic from DISH's RAN edge to its core network in AWS Regions. Other similar solutions in the market include Microsoft's Azure ExpressRoute and Google Cloud Interconnect.[43]

RAN

The move towards cloud-native virtualization is expected to increase the level of virtualization of components in Open RAN. This suggests that NFV and SDN will be very important in Open RAN. Open RANs are expected to rely heavily on cloud infrastructure as the virtual machines (VM), on which the applications that provide the functions of CU and DU are run, will reside in the cloud, more specifically RAN Edge cloud.

In fact, in the cloud-native approach, VMs are replaced by containers, which allow users to package software (e.g. applications, functions, microservices) with all the necessary files to run it and at the same time share access to the operating system and other server resources.[44] The contained component can be moved between environments such as clouds.

[43] https://www.megaport.com/blog/comparing-cloud-providers-private-connectivity/
[44] https://www.redhat.com/en/topics/cloud-native-apps/vnf-and-cnf-whats-the-difference

This means cloud-native Open RAN implementations are collaborative between RAN hardware suppliers, software suppliers and cloud infrastructure providers. This contrasts with a legacy RAN, where all dedicated hardware and built-in software are supplied by a single vendor such as Nokia, Ericsson and Huawei. Virtualization and the deployment of Open RAN, therefore, result in a disaggregation of the market for supply of RAN.

RAN edge

The RAN edge is a direct product of virtualization. In the traditional model, where the BBU and the RRH were bundled in a single kit, signal processing takes place at the cell site. The RAN edge of more evolved RANs is necessitated by the virtualization of functions performed by the BBU in a traditional network. The RAN edge has also made it possible for more demanding services, in terms of speed, bandwidth and latency, to be provided.

The introduction of RAN edge to the RAN, thus, creates a new market for supply of edge computing. MNOs need to install servers and data centres, which are procured from hardware and software suppliers such as DELL. MNOs' deployment of RAN edge, in turn, creates a market for supply of MEC services (and other RAN-edge cloud services), which are based on a cloud provider's infrastructure co-located with MNOs' RAN edge nodes.

However, some caution is necessary, because so practical implementations of the edge computing have been limited. Cooperation models between cloud providers and mobile network operators so far appear to keep the servers in data centres up to several hundred kilometres away from the consumer. This is quite different than the visionary predictions of having a small data centre in each antenna site. It is yet unclear if newer generations of services need even lower latency and therefore demand edge computing in the RAN, or if the computing will remain on device and in a regional data centre further away.

5.2.3 Network operations

Cloudification and virtualization of the Infrastructure and Network equipment building blocks has led the evolution of market players in the Network Management building block.

Traditional OSS solutions providers have shifted from on-premises software solutions to cloud-based solutions offered as SaaS. These rely on a third-party cloud provider such as AWS or Microsoft. The market has also seen the emergence of new players who offer cloud-native solutions built in micro applications, such as Amdocs.

5.2.4 Business support

Compared to the traditional ECN/S model (Section 3), the categories of BSS market players have evolved and expanded with the cloudification of networks. The shift towards cloud-based architectures and technologies has influenced the BSS market ecosystem, leading to the emergence of new players and altering the roles of existing ones.

- BSS solution providers: The cloudification of networks has facilitated the rise of BSS as a Service (BSSaaS) providers. These companies offer pre-built BSS solutions hosted in the cloud, which telecom operators can subscribe to and access as a service. BSSaaS providers handle the infrastructure, maintenance, and updates, enabling operators to focus on their core business.

- System integrators and managed services: With the cloudification of BSS, managed service providers (MSPs) and system integrators play a crucial role in assisting telecom operators with the migration, integration, and management of their cloud-based BSS systems. They offer services such as cloud infrastructure management, system integration, customization, data migration, and ongoing support, ensuring smooth operations and optimal performance. We would also include in this category consulting and advisory services: Because the cloudification of networks has increased the complexity and strategic implications of BSS transformations for telecom operators, some consulting firms have specialized in cloud-based services to assist operators in formulating cloud strategies, assessing vendor options, identifying business benefits, and designing migration roadmaps. They provide guidance on leveraging cloud technologies effectively to achieve desired business outcomes.

- Cloud Service Providers: With the cloudification of networks, cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform have become prominent players in the BSS market. They offer cloud infrastructure, platform services, and software-as-a-service (SaaS) solutions that telecom operators can leverage to deploy their BSS systems in the cloud.

- Specialist providers have evolved or emerged:

    - Security and Compliance Providers: Cloud-based BSS systems require robust security measures to protect sensitive customer data and comply with regulatory requirements. Security and compliance providers cater to the specific security needs of telecom operators in the cloud environment. They offer solutions and services such as cloud security assessments, identity and access management, data encryption, and compliance audits.

    - Data analytics and AI providers: The cloudification of networks has enhanced the capabilities of data analytics and artificial intelligence (AI) in the BSS domain. Specialized players have emerged, providing advanced analytics solutions, machine learning algorithms, and AI models specifically tailored for telecom operators' BSS data. These providers help operators derive actionable insights, predict customer behaviour, optimize pricing strategies, and enhance revenue management.

Examples of BSS market players include IBM, Amdocs, Nokia, Oracle, Ericsson, HP, Cisco, Cap Gemini, Huawei, NET Cracker, Accenture, Infovista, ComViva, and STL. Some players operate in some geographical regions like Alepo (US, South America, India). The cloud has expanded the ecosystem, creating new opportunities for specialized providers and changing the dynamics of the BSS market by offering scalable, flexible, and cost-effective solutions to telecom operators.

5.2.5 Development of strategic partnerships and collaborations

The research shows that the current model of ECS provision relies on a complex ecosystem of players, comprising traditional electronic communication services providers, cloud infrastructure and services providers, traditional equipment vendors and cloud-native software vendors and integrators. Strategic partnerships and collaborations are being forged between the different players.

First, partnerships have developed among cloud-based vendors, suppliers and providers[45], particularly for OSS and BSS services. Companies like Netcracker Technology (NEC Corp) and Amdocs have closed deals with Microsoft Azure[46][47] and Google Cloud[48][49] to offer BSS/OSS applications on their platforms. Ericsson and AWS have partnered on Cloud BSS[50].

Second, strategic collaborations can also be noted between cloud-based vendors, suppliers and providers with CSPs.

- Telefónica and Oracle[51] jointly offer platform-as-a-service (PaaS) and applications to enterprises and public sector organisations. The global partnership enables Telefónica to offer B2B customers an on-ramp to Oracle Cloud Infrastructure supporting them with its own portfolio of managed and professional services.
- Microsoft has acquired Network Cloud platform of AT&T (June 2021); the agreement includes the migration of the AT&T 5G core network to Microsoft's cloud. This has happened following Microsoft acquiring Affirmed Networks[52], American specialist of

[45] Vendors refer to manufacturers and sellers of network equipment. Suppliers are firms that that supply solutions that may comprise both hardware and software. Providers denote firms that primarily provide software or data-based service or managed software/data-based service through their own physical infrastructure.

[46] 2020 (https://www.netcracker.com/news/press-releases/netcracker-offers-ai-driven-digital-bss/oss-to-microsoft-azure.html)

[47] 2021(https://www.amdocs.com/news-press/amdocs-expands-strategic-collaboration-microsoft-boost-service-providers-journey-cloud)

[48] 2020(https://www.netcracker.com/news/press-releases/netcracker-and-google-cloud-announce-strategic-partnership-to-help-telcos-modernize-business-and-operational-systems.html)

[49] https://www.amdocs.com/about/partners/google-cloud

[50] 2021 (https://www.ericsson.com/en/blog/2021/5/ericsson-and-aws-partner-to-support-csps-on-their-journey-to-cloud-bss)

[51] https://telecoms.com/513428/telefonica-tech-and-oracle-strike-global-cloud-deal/

[52] https://www.usine-digitale.fr/article/microsoft-acquiert-affirmed-networks-specialiste-de-la-virtualization-des-reseaux-5g.N946776

cloudification of 5G networks, and Metaswitch Networks[53], virtualization software provider.

- T-Mobile has a partnership with Netcracker on its billing platform for its wholesale business[54].
- Virgin Media O2 selecting Mavenir on its Open RAN deployment is another example of market collaboration.[55]
- Edge Computing services. The possibility of bringing a public cloud's capabilities closer to the users through the RAN edge has also spurred partnerships between cloud providers and MNOs. In many markets, MNOs and cloud providers collaborate on Multi-access Edge Computing services (MEC). Ericsson & Telstra have developed an enterprise edge cloud solution with an extension into the hybrid cloud space[56]. In Germany, 2020 article says O_2 Telefónica[57] partners with AWS and Ericsson, whereas 2022 article describes the partnership of O_2 Telefónica[58] with Google Cloud and Ericsson.

Finally, CSPs have partnered among themselves. Orange and Vodafone[59][60] have announced their Open RAN sharing agreement (2023) with a pilot in Romania and a large-scale deployment objective in 2025. In a Memorandum of Understanding (MoU) dated February 2023[61], Deutsche Telekom, Orange, Telecom Italia, Telefónica, and Vodafone have set out their agenda for the year under the three main topics of maturity, security, and energy efficiency. In early 2021, they had individually committed to working with all industry players to make Open RAN the technology of choice for future mobile networks.

The moving and dynamic market of cloudification of ECN/S is reflected in the partnerships that have been closed so far. Market dynamics are becoming more complex as players are involved in different parts of the value chain.

[53] https://www.usine-digitale.fr/article/microsoft-acquiert-metaswitch-networks-pour-se-renforcer-dans-la-virtualization-des-reseaux.N965181

[54] https://www.netcracker.com/news/press-releases/netcracker-extends-strategic-relationship-with-t-mobile,-america%E2%80%99s-5g-leader.html

[55] https://news.virginmediao2.co.uk/6561-2/

[56] https://www.ericsson.com/en/press-releases/2020/11/ericsson-and-telstra-collaborate-on-edge-cloud-for-enterprises

[57] https://www.telefonica.de/news/press-releases-telefonica-germany/2020/09/cooperation-with-amazon-web-services-and-ericsson-drives-new-industrial-5g-solutions-telefonica-deutschland-o2-builds-its-new-5g-core-network-in-the-cloud.html

[58] https://www.telefonica.de/news/press-releases-telefonica-germany/2022/12/network-of-the-future-for-new-5g-solutions-o2-telefonica-lifts-5g-core-network-into-the-cloud-to-unlock-new-opportunities.html

[59] https://www.silicon.fr/open-ran-premier-elan-europe-459068.html

[60] https://www.datacenterdynamics.com/en/news/orange-and-vodafone-pen-open-ran-sharing-agreement/

[61] https://newsroom.orange.com/major-european-operators-accelerate-progress-on-open-ran-maturity-security-and-energy-efficiency/

6. Practical considerations for deployment of these technologies

6.1 Flow of data between systems and integrity of APIs

An Application Programming Interface (API) is a group of protocols and methods that define how two applications share and modify each other's data. In effect, an API is a set of rules that allows a software program to communicate with another software program.

An API is located between a software's core components, which provide the functionalities, and the public. External developers can access certain parts of an application's backend without the need to understand how everything works inside the software. This means APIs can also be used by developers to avoid having to code from scratch application functions that already exist elsewhere. Developers can incorporate existing APIs into their new applications by formatting requests as the API requires, instead of creating new application functions that perform the same tasks.[62]

6.1.1 Types of APIs

There are established frameworks for creating APIs. The common framework is REST (Representational State Transfer). APIs that conform to REST are called REST APIs. REST APIs are the most common type of API used for cross-platform integrations as well as in microservices.[63]

REST defines a set of constraints for API development that make them efficient and secure. REST APIs work by making requests over HTTP (Hypertext Transfer Protocol) format and returning responses, typically, in JSON (JavaScript Object Notation) format. HTTP is already the standard protocol for web-based data transfer, making it easier for developers to learn how to build or interact with a REST API.

In addition, APIs can be both open and private. Open APIs are available for anyone to use, including third-party software developers. Open APIs are being widely used by MNOs to expose the functionalities of their virtualised networks to developers. Early in 2023, the GSMA launched an industry-wide initiative called GSMA Open Gateway. This framework of universal network API is supported by 21 mobile network operators with the objective to provide universal access to operators' networks for developers and cloud providers[64]. Orange, for example, announced its drive to open its network to service developers through APIs at the MWC23,[65] and the Linux Foundation CAMARA project which was set up to define, develop

[62] https://www.cloudflare.com/en-gb/learning/security/api/what-is-an-api/

[63] https://www.ibm.com/topics/rest-apis#:~:text=the%20next%20step-,What%20is%20a%20REST%20API%3F,representational%20state%20transfer%20architectural%20style.

[64] https://www.gsma.com/futurenetworks/gsma-open-gateway/

[65] https://hellofuture.orange.com/en/apis-move-closer-to-the-core-of-the-network/

and test APIs, is also part of this initiative. The idea is that such network APIs will help to unlock technical capabilities in industries through the use of the MNOs' networks.

Private APIs, on the other hand, has access restrictions and are used for communication within an application. Access is usually limited to an organisation's employees and authorised developers and not openly accessible to the public.

6.1.2 Issues around APIs in a virtualised, softwarised and cloudified network

APIs and microservices

APIs are necessary in modern digital infrastructure, as they enable streamlined communication between applications, including virtual machines, which might differ in function and construction. As explained earlier in this report, the process of virtualization and cloudification of network has led to the deployment of virtual machines, which, in turn, are gradually being replaced by containerised microservices due to their agility.

Microservice architecture involves building an application as independent components that run each application process as a service. These services communicate with each other via a well-defined interface using lightweight APIs.[66] In fact, containerised microservices communicate with each-other via standardised RESTful APIs. This means that such APIs for microservices will need to be secure and efficient, while remaining open to ensure that the systems function properly.

API and vendor lock-in

One of the advantages of virtualization is the possibility to avoid vendor lock-in. Proprietary software and hardware that provides network functions can be replaced by COTS hardware and VNFs. However, to build an integrated system, VNFs still need to be able to communicate with each other. VNFs communicate with each other using APIs.

The use of private APIs by a vendor would mean that they are not discoverable or accessible to third-party VNF vendors, which could result in a lack of interoperability between VNFs. This resulting lack of interoperability would make it difficult for the MNO to mix and match solutions. This also gives rise to the possibility of vendor lock-in. A vendor could make all the APIs internal to their VNFs, and only its own VNFs can communicate with each other. An MNO that chooses one VNF from the vendor will be forced to use other VNFs from the same vendor by default.[67] This highlights the importance of API openness.

Additionally, Physical Network Functions (PNFs) continue to represent a large part of MNOs' networks; NFV is being implemented incrementally in the core network and RAN of these

[66] Lightweight APIs refer to APIs that have a small memory footprint and are easy to implement.
[67] https://www.itential.com/blog/company/network-cloud-automation/apis-nfvs-holy-grail-of-interoperability/

operators. As such, many MNOs networks still rely on many proprietary, physical hardware devices that are complex to operate and difficult to integrate because of their vendor-specific APIs. Challenges also remain in connecting these APIs with open-source orchestration systems, such as Kubernetes, an open-source container orchestration system.[68] This could continue to hamper effort to move toward a disaggregated model of equipment supply.

Cloud API

In the traditional model, where all network components are owned and operated by the MNO, data does not move across the boundary of the MNO's domain until it connects to the internet through a gateway. Data processing takes place within the MNO's own infrastructure. This is also the case where a virtualised network is built on a private cloud that is owned and operated by the MNO.

It is possible that multiple clouds, both private and public, are used for a virtualised network. This is where there may raise issues around APIs. Functionalities and services of a public cloud, such as computing and storage, that are needed to construct VNFs, are accessible through cloud API. Cloud APIs connect services within cloud environments. However, they may not be compatible with every cloud provider or not be built to work across different cloud providers' environments.[69]

Vendor-specific cloud APIs are designed to work with services from a single cloud provider. This contrasts with cross-platform cloud API, which is compatible with multiple cloud providers. The use of vendor-specific cloud APIs by a cloud provider could therefore have the effect of locking in the MNOs to this provider. Switching from a cloud environment to another would require a new API, which has implications for the ease with which an MNO can pick and choose services in different clouds to optimise its network.

6.2 Data storage and processing

To provide good quality services and customer experience, and to manage networks and distribution of content and services well, electronic communications providers must be able to manage a range of data efficiently. These include customer data, data about consumption and service preferences, service data, data for network and service management OSS and BSS functions.

Storage is a key component of data management. As the volume of communications services and data transmission increase, so does the need for secure, reliable, and resilient data storage in the provision of electronic communications networks and services. This is a trend which is expected to continue as 5G and very high-performance fibre networks support the

[68] https://dgtlinfra.com/network-functions-virtualization-nfv/

[69] https://www.cloudflare.com/en-gb/learning/security/api/what-is-a-cloud-api/

transmission of greater volumes of data, and hence also create demand for increased capacity and future scalability of data storage.

6.2.1 Cloudification of data storage

Traditionally, data has been stored in large data centres. The physical location of such data centres can be challenging for efficient data management to meet the needs of modern communications and data transfer. In large organisations, data storage can also be organised in a siloed manner according to different products or brands within a company, or according to the structure of the organisation. This can make flexible access to data difficult, but increasingly modern services demand it.

6.2.2 Distribution of data storage – edge storage

The development of new services requiring high-speed data transmission and ultra-low latency also requires very efficient access to and transfer of data. This is already the case for both consumer and business use cases and will become increasingly so in the near and medium-term future. The speed and efficiency of data transfer will become critical as digital technology is deployed to deliver applications requiring near instantaneous data transfer such as automated transport systems, and remote digital healthcare capabilities.

Transmission and access networks are already able to handle high speed transmission of data, and the accelerated development of fibre-to-the-premises (FTTP) and high-speed capability of 5G (and eventually 6G) are providing further components of the infrastructure to deliver ultrafast and very high-quality capabilities.

Another key part of the ecosystem to deliver higher speed and more reliable data transfer is data storage using more distributed models of data storage, i.e. moving data away from centralised silos in data centres to more flexible facilities closer to the customer or source of data. This improves the efficiency of data transfer in both directions. As noted though in Section 5.2.2 though, the migration of data storage to the edge of telecoms networks has not developed in the way some expected. It remains to be seen whether the need for lower latency use cases drives faster development of edge data storage as full fibre and 5G networks are deployed.

6.2.3 Cloudification at the edge

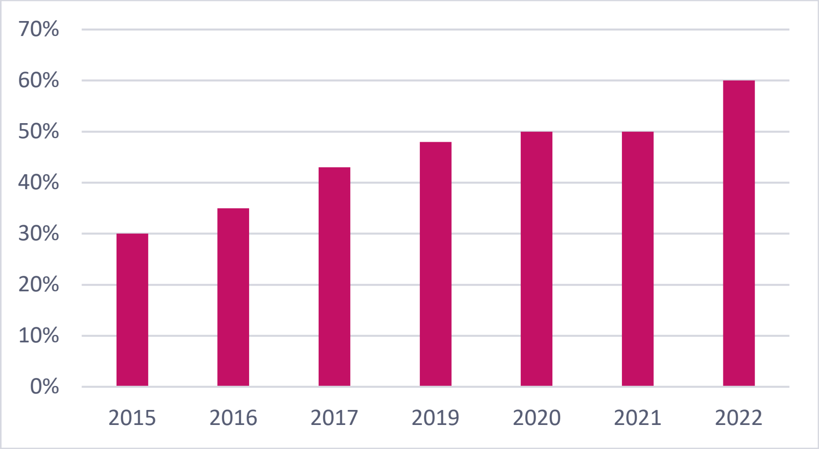
Cloudification of data storage is a feature of this transformation.

Cloudification can make it easier for providers to combine data from a number of sources and this can help to make BSS functions more flexible, for example, responding to customer preferences by offering increased personalisation of customer propositions. It also has the potential to improve the scalability of data storage without requiring more data centre space. Hence, the move to more distributed models of data storage and management in the cloud are a feature, not just of electronic communications networks and services, but of many services and logistics in sectors across the economy.

6.2.4 Practical considerations of cloudified data storage

Digital transformation means that, overall, companies create, process and store more data in the cloud than ever before. This trend is forecast to continue.[70]

Figure 6.1: Share of corporate data stored in the cloud



Source: Statista, note data unavailable for 2018

ECS providers see particular advantages to edge-based cloudified data storage because it enables flexible data management and efficiency in data transmission closer to the customer. Providers are managing a number of considerations to facilitate the benefits of cloudified data storage. These include:

- Greater flexibility and scalability as data storage needs continue to evolve and increase.
- Environmental externality benefits of reducing carbon emissions in cloudified data storage relative to physical data centres. Telecom companies estimate that cloud deployments (in data storage and communications) will reduce greenhouse gas emissions by 5%.[71]
- Management of data security in cloudified environments. The migration to cloud-based solutions involves management to ensure data security is not compromised and that data

[70] See for example https://www.fortunebusinessinsights.com/cloud-storage-market-102773
[71] https://www.techradar.com/news/telcos-are-set-to-spend-billions-on-new-cloud-infrastructure

storage and processing complies with all legal and regulatory requirements and meets industry standards. In interviews carried out for this study, ECN and ECS providers and cloud infrastructure providers stated that maintaining or improving data security is a key consideration (a “non-negotiable”) in cloudification.[72]

6.3 Security of infrastructure & networks

While the virtualization, softwarization and cloudification of telecommunications networks offer numerous benefits, it also raises several security issues across the ECS provision value chain. This means that telecom operators as well as other players such as the equipment vendors, the software providers and the cloud providers have to face several challenges to accelerate the virtualization, softwarization and cloudification of telecommunications networks.

Each technology covered in this report introduces its own set of security issues. Besides, stakeholders have to tackle specific security aspects across the different building blocks. Nevertheless, there are common issues impacting the whole value chain including the following:

- An increased attack surface: As more software is introduced in the networks, the vulnerabilities that need to be patched are increased. For example, cloud based environments may have more interfaces and APIs. Additionally, many vendors and operators rely on open-source software as development processes often incorporate the use of prebuilt and reusable open-source software components. When open source is used as the foundation for a vendor’s product, any vulnerabilities could threaten the integrity of the vendor’s solution.

- Shared infrastructure risks: In virtualized and cloud environments, telecom operators often share physical resources, such as servers, storage, and network infrastructure, with other tenants. Inadequate isolation between tenants can lead to potential attacks, such as unauthorized access, data leakage, or lateral movement[73]. Implementing strong isolation mechanisms, network segmentation, and access controls is essential to mitigate shared infrastructure risks.

- Shared responsibility for security between cloud providers and their customers can create complex accountabilities and risks.

- Multi-vendor environment: With the containerisation and the emergence of new players, telecom operators now rely on a complex supply chain of vendors and service providers for virtualization and cloud solutions. This multi-vendor environment makes the

[72] For example, the General Data Protection Regulation (GDPR) requires storage of data within the European Union, see https://commission.europa.eu/law/law-topic/data-protection/eu-data-protection-rules_en

[73] Lateral movement refers to the techniques that a cyber attacker uses, after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets.

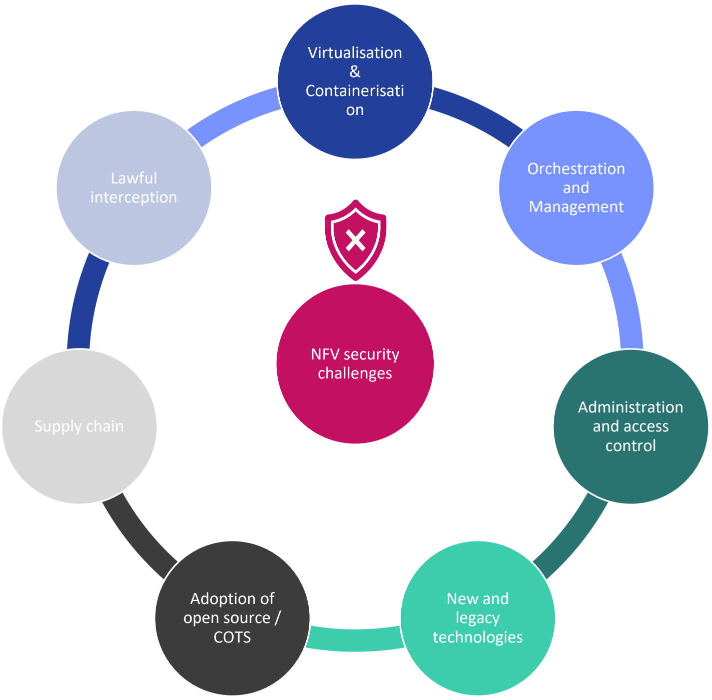
coordination of security policies more complicated and requires more effective network security monitoring capabilities.

- Supply chain risks: Compromised, counterfeit or malicious components within the supply chain, poor designs and manufacturing processes can have negative consequences such as loss of confidence in the network integrity or system and network failure. Thoroughly vetting vendors, conducting security assessments, and establishing strong contractual agreements are essential to mitigate supply chain risks.

6.3.1 Focus on NFV Security challenges

NFV technologies fostered by the development of 5G networks introduce several security challenges not only for operators but for all the market players. These may include increased attack surface, shared responsibility risks, and supply chain risks. The European Union Agency for Cybersecurity has developed a taxonomy of NFV-related risks[74] that identify 60 security challenges grouped into 7 categories. These categories are presented in Figure 6.2 below. To help mitigate these challenges and improve NFV security, ENISA has also established fifty-five policy, technical and organisational best practices.[75]

Figure 6.2: NFV security challenges


Virtualisation & Containerisati on
Orchestration and Management
Administration and access control
New and legacy technologies
Adoption of open source / COTS
Supply chain
Lawful interception
NFV security challenges

Source: ENISA

[74] https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices

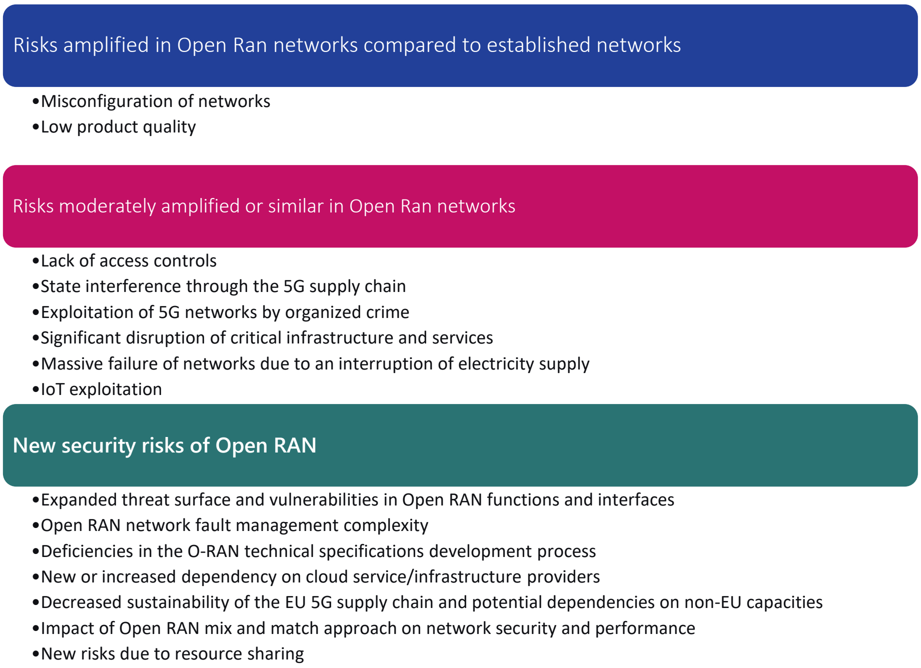
[75] A detailed description of security challenges and best practices is available here: https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices

6.3.2 Focus on Open RAN security challenges

Open RAN is still an emerging concept that is rapidly evolving which means that there is still uncertainty around usage scenarios and technical specifications, particularly when it comes to security[76]. While it offers higher agility, and flexibility in telecommunications networks, it also introduces new security considerations for operators. The model of ‘Openness’ that implies an entire ecosystem of disaggregated multi vendors raises specific challenges related to integrating components from multiple providers, the use of open-source applications and new 5G network functions and interfaces.

The European Commission published a report[77] on Open RAN security that listed potential risks of strategic importance from an EU perspective. Some of these risks are similar in Open RAN networks compared to traditional networks such as the potential lack of access control or the network failure due to an interruption of electricity supply. Some risks, such as the misconfiguration of networks and the low product quality are amplified in the context of Open RAN networks. Additionally there are new security risks specific to Open RAN that have also been identified. There risks are shown in Figure 6.3 below.

Figure 6.3: Open Ran security challenges



Risks amplified in Open Ran networks compared to established networks

- Misconfiguration of networks
- Low product quality

Risks moderately amplified or similar in Open Ran networks

- Lack of access controls
- State interference through the 5G supply chain
- Exploitation of 5G networks by organized crime
- Significant disruption of critical infrastructure and services
- Massive failure of networks due to an interruption of electricity supply
- IoT exploitation

New security risks of Open RAN

- Expanded threat surface and vulnerabilities in Open RAN functions and interfaces
- Open RAN network fault management complexity
- Deficiencies in the O-RAN technical specifications development process
- New or increased dependency on cloud service/infrastructure providers
- Decreased sustainability of the EU 5G supply chain and potential dependencies on non-EU capacities
- Impact of Open RAN mix and match approach on network security and performance
- New risks due to resource sharing

Source: European Commission

Further work has been done to understand security risks arising from Open RAN (i.e. which are unique to Open RAN). In its May 2023 Open RAN Security Report, the Quad Critical and

[76] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks
[77] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2881

Emergency Technology Working Group[78] found that 4% of security risks identified for 5G networks are unique to Open RAN.[79] The same report also identified some relative security advantages in Open RAN. The UK Government has identified vendor diversity as an opportunity for more openness and scrutiny enabling potentially better detection of security risks.[80]

Discussions with network operators revealed that addressing security issues are key for the future of Open RAN and its deployment, with stakeholders telling us that robust security is a key pre-requisite to the deployment of Open RAN.[81] Although there have been some examples of deployment, it appears that many operators are not willing yet to take the risk of adopting a full Open RAN network. On the other hand, there appears to be a strong concern regarding the ‘balkanisation’ of security requirements as different countries, regions and organisations are developing different security standards.

6.3.3 The EU toolbox of 5G cybersecurity risk mitigating measures

Following the call of the European Council on 22 March 2019 for a concerted approach to the security of 5G networks, the European Commission adopted its Recommendation on the cybersecurity of 5G networks on 26 March 2019. The Recommendation called on Member States to complete national risk assessments and review national measures, to work together at EU level on a coordinated risk assessment and to prepare a toolbox[82] of possible mitigating measures.

The main objective of the toolbox is to identify a common set of measures to mitigate the main cybersecurity risks of 5G networks as they have been identified in the EU coordinated risk assessment report, and to provide guidance for the selection of measures which should be prioritised in mitigation plans at national and at Union level.

6.4 Sustainability in cloudification

6.4.1 Sustainability as a core matter throughout the ecosystem

Sustainability is a core focus of stakeholders interviewed for this report. The concept is large, as, according to the definition it is given in the context of electronic communications, it may cover digital inclusion (enabled – among others - by geographical coverage and provision of affordable services), where digital services can aid in a more sustainable society, as well as

[78] The Quad is a partnership between the USA, Australia, Japan and India.

[79] https://ntia.gov/sites/default/files/publications/open_ran_security_report_full_report_0.pdf

[80] https://www.gov.uk/government/publications/uk-open-ran-principles/open-ran-principles

[81] This position was explained by stakeholders in interviews for this project with Plum and Stratix.

[82] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

the environmental impact of the networks themselves. The concept may be tricky as improving coverage to foster digital inclusion may negatively impact the environment.

Digital sustainability involves reducing energy, raw materials usage and in general resources consumption. Also cross effects and interdependencies between the operations of ecosystem's stakeholders have been underlined in the Arcep-ADEME report[83]: "This distribution of impact must not, however, make us lose sight of digital's eco-systemic dimension: the interdependence between devices, networks and data centres created by consumption must be taken into account when drafting public policies targeting the digital environmental footprint as a whole."

For network operators the scope 2 emissions are often the largest source of their operational emissions, through the electricity they purchase. Reducing the electricity use is an aim in cloudification, through a larger shared use of resources for different tasks. In the networks the move to fibre-based networks and copper shutdown helps in reducing absolute energy consumption. The increase in the number of mobile sites to improve coverage and performance of networks can lead to increases in absolute energy consumption. Virtualising RAN components may then help in sharing some equipment and lowering consumption. Some of the savings are achieved in an indirect way: when parts of the network are designed to consume less electricity, they create a virtuous circle of smaller electricity supplies, back-up batteries and cooling systems.

One of the interviewees underlines that the most important part of their CO2 emissions is Scope 3[84] meaning indirect emissions produced by their procurement (suppliers) through the production and installation of equipment. When equipment can be used for longer periods or re-used elsewhere, this decreases the scope 3 emissions. In addition, because field operations are mostly outsourced, operators are looking to reduce the number of their interventions and to make them minimize the impact per intervention through specific vendor selection requirements. An interviewee mentioned that as an incentive, 20% of procurement score in the sourcing process is dedicated to the environmental impact of the bidder. Market players also move towards more energy-efficient infrastructures with the use of renewable energy on radio sites[85] (local solar panels or wind turbines).

Industry and regulatory incentives that drive and impact cloudification

Cloudification is in part also driven by sustainability requirements and reporting. Aggregating equipment in datacentres with higher efficiency and utilisation lowers the overall energy consumption and can lead to direct and indirect savings. Older datacentres and regional sites may have had Power Use Efficiency (PUE) ratios of above 2, which means that for each 100W

[83] https://www.arcep.fr/la-regulation/grands-dossiers-thematiques-transverses/lempreinte-environnementale-du-numerique/etude-ademe-arcep-empreinte-environnemental-numerique-2020-2030-2050.html
[84] https://ghgprotocol.org/sites/default/files/standards_supporting/FAQ.pdf
[85] https://www.ericsson.com/en/news/2021/2/dt-sustainable-mobile-sites

used by computing and network equipment they needed more than 100W for cooling, back-up power etc. Modern datacentres have PUE's below 2. The 2023 EU Energy Efficiency Directive sets targets for new and existing datacentres to have PUE's below 1.3, meaning that for each 100W of computing and networking equipment only 30W in cooling, back-up power etc. is allowed.[86] For ECN/S providers this means that by 2030 some of their datacentre locations must comply with these regulations.

Following the EU's Green Deal that sets up environmental targets for the EU, cloud providers and data centres operators have decided to apply self-regulation. The Climate Neutral Data Centre Operator Pact[87] was launched in 2021 and now has over 100 signatories representing over 90% of data centre capacity offered in Europe. It is a collaboration between stakeholders that aims to achieve climate neutrality by 2030 based on the following commitments:

- Increase and measure their efficiency,
- Using renewable energy at 75 percent of their consumption (some signatories have committed to a higher target),
- Addressing water efficiency,
- Taking part in a circular economy to repair and recycle servers,
- Reusing waste heat where possible,
- Using the PUE (Power Usage Effectiveness) standard[88],
- Looking at creating a new metric to replace the aging PUE standard.

A Pact approved third-party assurance firm will certify these efforts and reassess them every four years. A penalty for failure to these commitments is the expulsion from the Pact behind the agreement. Losing the stamp of approval may lead to losing clients. As more ECN/S move to cloud services provided by signatories of the Pact, the share of the sector's energy use powered by renewable energy will increase.

The attitude of their customers and governments towards digital sustainability has become a core consideration of IT business decision makers as well as a must-have and a potential deal-breaker in business relationships. Suppliers to ECN/S providers, the ECN/S providers themselves and their customers all emphasize the sustainability aspects involved in the purchase of goods and services.[89] However, some interviewees did mention that because

[86] Directive (EU) 2023/1791 of the European Parliament and of the Council of 13 September 2023 on energy efficiency and amending Regulation (EU) 2023/955 (recast) https://energy.ec.europa.eu/topics/energy-efficiency/energy-efficiency-targets-directive-and-rules/energy-efficiency-directive_en

[87] https://www.climateneutraldatacentre.net/

[88] https://www.techtarget.com/searchdatacenter/definition/power-usage-effectiveness-PUE

[89] As an illustration the websites of Ericsson and Nokia have large sections emphasizing the energy efficiency of their products and services https://www.ericsson.com/en/about-us/sustainability-and-corporate-

electricity prices have risen and are therefore a larger part of total cost of ownership, the sustainability benefits of reduced electricity consumption are an additional benefit rather than the primary driver.[90]

Cloud is expected to play a critical role in datacentre sustainability. The cloudification of ECN/S is seen as having clear benefits on the energy consumption part. However, the exact environmental impact of cloudification is a topic of considerable debate. Some analysts expect a rebound effect: if digital services are perceived as greener, users are more inclined to consume them. This effect known as the Jevons Paradox[91], is however not apparent with consumer applications. Complicating the debate is that there is currently no standardised way of reporting on the resource use (electricity, water, minerals) by the digital sector. Most academic and industry analyses on energy and water consumption are extrapolations based on averages of a few examples, leading to large variations in estimates.[92] The Energy Efficiency Directive will require datacentres to report on their resource use from 2024 onwards. Analysis is also complicated because many ECN/S providers, their suppliers and customers have only recently started reporting on their resource use and may not include the resource use when workloads are moved to suppliers or cloud-computing firms. Which means that when a database is moved from a server owned and operated by an ECN/S firm to a cloud service of a supplier the reduction in energy consumption is recorded, but the increase in energy consumption of the cloud service of the supplier isn't visible. The complexities of such metrics are outside the scope of this report.[93]

6.4.2 Direct sustainability benefits of ECN/S cloudification

Cloudification and virtualization of ECN/S is expected to enable:

- Less waste generation: A lower physical hardware footprint through virtualization and infrastructure sharing leading to less electronic waste;

- An optimized utilization of resources: On-demand auto-scaling of network via a dynamic allocation and re-allocation of resources enables to avoid overprovisioning and

responsibility/environment/product-energy-performance and https://www.nokia.com/networks/bss-oss/ava/energy-efficiency/.

[90] That sustainability is important, but not yet the most important in ECN/S is also remarked in this overview of the IBC2023 by the Greening of Streaming, https://theflint.media/the-greening-of-ibc-maybe-next-year/

[91] In 1865, the English economist William Stanley Jevons observed that technological improvements that increased the efficiency of coal use led to the increased consumption of coal in a wide range of industries. https://en.wikipedia.org/wiki/Jevons_paradox

[92] David Mytton, Masaō Ashtine, Sources of data center energy estimates: A comprehensive review, Joule, Volume 6, Issue 9, 2022, https://doi.org/10.1016/j.joule.2022.07.011

[93] Stratix research for the Metropole Region Amsterdam (MRA) found some striking examples on the complexity of getting accurate facts and figures on datacentres, clouds and networks. When the Dutch government or financial sector moved activities from inhouse server rooms to colocation datacentres around Amsterdam, the Central Bureau of Statistics records a reduction in energy consumption for the financial and public sector and an increase in energy consumption for the ICT-sector. That the reductions and increases are related is not apparent. Cf. Rapportage Datacenters, Impact en feiten, Stratix 2023, available at https://www.metropoolregioamsterdam.nl/feiten-en-fictie-rond-datacenters-ontrafeld/

underutilization of resources and the associated improved energy consumption. Use of AI and data indeed optimizes deployment and operations, like for example the prediction of low data traffic and turn-off of corresponding base stations, bringing tangible savings in the field;

- Fewer on-site visits: Remote management and troubleshooting of network issues through NFV and SDN reduces the need for on-site visits (and associated travel emissions).

For instance, telecom operators that have moved to cloud expect to reduce their greenhouse gas (GHG) emissions in the next 3-5 years.[94]

Overall, considering that cloudification of ECN/S is still being at a nascent operational stage, stakeholders we spoke to could barely provide inputs on the related sustainability topic besides theoretical expectations. They still do not have concrete and proven use cases to share for now but are confident in the sustainability potential of ECN/S cloudification.

6.4.3 Private vs. public cloud: different impacts on sustainability

Because they operate on different business models, private and public clouds do not have similar levels of impacts on the environment[95].

Efficiency. Large scale of operations of public cloud providers enables them to have resources to invest in energy-efficient infrastructure and innovative cooling technologies. They can distribute workloads more efficiently across their servers, which reduces the amount of energy wasted on idle resources. In contrast, private clouds, which are often smaller, may not have the same resources to invest in efficiency and may have lower utilization rates, leading to potentially higher per-unit energy use, calculated as Power Usage Effectiveness (PUE).

Infrastructure deployment impact. Public cloud infrastructures are usually large and centralized, whereas private clouds may be distributed across multiple smaller infrastructures. Building and maintaining the infrastructure for multiple data centres can have a larger environmental impact than a single, more efficient large-scale data centre.

Sustainable energy. Some public cloud providers have committed to using renewable energy for their data centres. If a company's private cloud uses electricity from the grid, it could have a higher carbon footprint than using a public cloud provider purchasing energy generated from renewable sources.

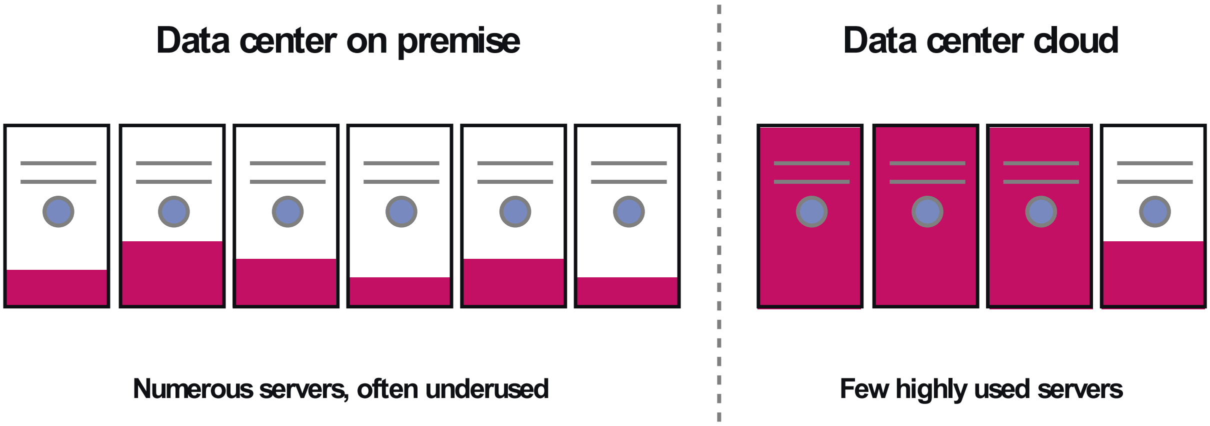
E-waste. Public clouds, because they pool resources among many users, can reduce electronic waste. Private clouds, on the other hand, may require more hardware per user

[94] Networks on cloud: a clear advantage, Capgemini Research Institute, Feb. 2023. The study focuses on the transition of wireless network functions (e.g. routers) and domains (RAN and core) to cloud-based infrastructure, in mobile networks.

[95] https://www.eescorporation.com/renewable-energy-and-cloud/

because they can't achieve the same economies of scale (Figure 6.4). This could lead to more e-waste as hardware becomes obsolete and is discarded.

Figure 6.4: Illustration of utilisation of servers in private cloud (left) vs. public cloud (right)



Source: Carbone 4[96]

Management of cloud resources is also important when considering the system’s sustainability. For example, a poorly managed public cloud could be more wasteful than a well-managed private cloud.

Hybrid cloud models can offer a balance between the efficiency of public cloud and the security and control of private clouds, and then be considered as a sustainable solution overall.

[96] https://www.carbone4.com/en/analysis-carbon-footprint-cloud

7. Overview of identified technological trends

This section summarises the main findings of our study of the technology evolution of the provision of ECN/S through cloudification, virtualization and softwarization. Impacts on market dynamics, competition and regulatory implications are then covered in Sections 8 and 9 of the report.

7.1 Evolution models

Virtualization of core network functions has been a feature of ECN development since the middle of the last decade. Combinations of generic hardware and virtualised network functions have enabled operators to deploy and manage more and more core network functions in the cloud. These deployments can be made on dedicated SDN Telco Cloud infrastructure. Alternatively, it is possible to deploy network functions in virtual private networks running on a public cloud.

Virtualised OSS and BSS systems are also deployed in the cloud, and hence cloud based systems are used to manage provisioning, deployment and scaling of services, and the billing and customer facing functions of BSS.

The development of virtualised and softwarised systems is not a generic concept, and each network deployment is different.

7.1.1. Open RAN, greenfield and brownfield

Open RAN is a good example of this because each network deploying Open RAN approaches it from a different starting point. Migration to Open RAN is more challenging for networks with consolidated legacy operations, hence early deployments have been mainly greenfield networks. For example, the Rakuten network in Japan is a pure Open RAN cloud native network (Rakuten-Symphony is also providing Open RAN solutions in other jurisdictions).[97] 1&1 is deploying a greenfield virtualised and cloud native Open RAN network in Germany.[98] DISH is deploying an Open RAN 5G network in the USA.[99]

Operators with established legacy networks are considering migration to Open RAN from a brownfield starting point. Early phases of deployment are sometimes geographically limited,

[97] https://global.rakuten.com/corp/about/

[98] https://www.1und1.ag/the-company#ueber-uns

[99] https://about.dish.com/company-info

or live trial environments.[100] Operators deploying or considering brownfield Open RAN deployments include Vodafone,[101] Deutsche Telekom, [102] and Virgin Media O2.[103]

Brownfield development perhaps reflects a risk-based approach to early adoption of technology. Phased deployments enable operators to address issues early before more widespread rollout, mitigate risks, and schedule milestones to gate key decisions. One approach to this more gradual integration of cloud based softwarised and virtualised solutions is to deploy them first in OSS and BSS systems as this is a lower risk environment than core or access network architecture.[104]

7.2 Developmental issues

Whilst there are real examples of cloud deployment in the ECN/ECS value chain, there is no single vision of how it will develop in the future. In interviews, it was reported that there is still a "wait and see" approach to cloudification in the access layer by some operators.[105] This is reflected in the phased brownfield Open RAN deployments described above, and in a rigorous approach to testing (see below).

The debate on deployment of Open RAN in 5G networks is at the centre of current industry focus on the development of cloudification in ECNs. Conceptually, Open RAN enables disaggregation of the RAN, opening the RAN environment to multiple vendors of software and hardware components. By its nature, this presents challenges in integration and coordination of components. Management and control of these disaggregated components is therefore important.[106] Complexity can create risk and, in the developmental phases of Open RAN, operators are considering the optimum level of disaggregation so as to ensure they can benefit by avoiding over-reliance or lock-in to vendors without creating a system with too much complexity.[107] The precise functional, software and vendor mix is likely to be different for each deployment, and this will increasingly be the case as innovators offer more customised solutions and bespoke consumer propositions.

Some of the risks of complexity can be mitigated by increasing automation throughout the deployment cycle, from testing to service delivery. Automation allows continuous testing and

[100] For example, Deutsche Telekom's "O-RAN Town" https://www.telekom.com/en/company/details/bundled-in-a-white-book-learnings-from-o-ran-town-1026846

[101] https://www.vodafone.co.uk/newscentre/press-release/switches-on-first-5g-openran-site/

[102] https://www.telekom.com/en/media/media-information/archive/first-commercial-open-ran-in-2023-1027618

[103] https://news.virginmediao2.co.uk/6561-2/

[104] This approach was described by a stakeholder in an interview for this project with Plum and Stratix.

[105] This approach was described by a stakeholder in an interview for this project with Plum and Stratix.

[106] For example, see https://www.mavenir.com/portfolio/mavair/radio-access/openran/

[107] This view was expressed by a stakeholder in an interview for this project with Plum and Stratix.

deployment at scale,[108] with human intervention only when it is needed (e.g. to manage flagged issues, and for final validation steps).[109]

The challenges of network transformation are not only technical. Different skillsets also are needed to manage less physical network environments, and the process of migration from physical to virtualised and softwarised functions.[110] In the evolved and future networks, ECN management may require more software, programming and AI skills than traditional field force engineering skills.

7.3 Testing

It (almost) goes without saying that effective testing is critical to the deployment of new technology. Extensive activity in test and live environments has been and is being undertaken and is currently an important feature of the Open RAN landscape. Likewise, robust testing is necessary to validate migration of network and operational functions from physical to cloudified, virtualised and software driven environments.

Deutsche Telekom's O-RAN Town live trial was a significant landmark in validation of OpenRAN. Deutsche Telekom documented and published its learnings in a White Paper.[111]

We spoke to a number of stakeholders who have undertaken or been involved in trials of Open RAN systems. They reported issues which they have needed to manage, some associated with the integration and compatibility of systems working together and multiple vendors. Such issues are not unusual in technology trials and one of the key purposes of trialling is to flush out and analyse such issues.

For Open RAN, testing is important at various points in the architecture and compatibility testing is needed between vendors. Hence, vendors and software provide open-source platforms for compatibility testing which can happen prior to more complex and bespoke systems integration. The O-RAN Alliance provides testing and integration facilities,[112] including "Plugfest" open trails.

As noted above, automated testing has facilitated progress at scale 24/7, improving efficiency of testing and mitigating risks.

[108] For example, see https://telecomreseller.com/2020/12/29/end-to-end-testing-and-what-it-means-for-telecoms/#:~:text=Automated%20testing%20allows%20for%20the%20integration%20of%20continuous,the%20development%20and%20maintenance%20of%20regression%20test%20suites.

[109] Automated processes were described as important to mitigate risks by a stakeholder in an interview for this project with Plum and Stratix.

[110] This view was expressed by a stakeholder in an interview for this project with Plum and Stratix.

[111] https://www.telekom.com/en/company/details/bundled-in-a-white-book-learnings-from-o-ran-town-1026846. As noted, Deutsche Telekom is moving on to operation deployment of O-RAN.

[112] https://www.o-ran.org/testing-integration

7.4 Standardisation

Standards are an important feature of electronic communications. Standards which are approved by a recognised standards body and adopted by industry have enabled communications ecosystems to develop with built in capabilities for interoperability and integration between systems. The Global System for Mobile Communications (GSM) standard is a good example of a highly successful standard that allowed for harmonisation and interoperability across 90% of the global mobile industry in the 2G era.[113]

Work has been underway on standards to harmonise network virtualization and softwarization since the middle of the last decade, and ETSI has established standards for NFV and SDN.[114]

Standards need to adapt as technology develops, and sometimes there can be lags between the pace of innovation and the careful and coordinated work needed to set standards. The landscape within which policy makers and standards organisations now face becomes more fragmented. Again, Open RAN is a good example. Open systems of disaggregated components mean coordination and standardisation are challenging. Technology and architecture are nascent. Careful coordination is therefore needed between commercial deployment, testing and standardisation of key interfaces to ensure networks are secure, sustainable and interoperable.

There can be added complexity because brownfield deployments require interoperability between new components and legacy systems.[115]

For Open RAN, work is underway in the O-RAN Alliance,[116] 3GPP,[117] ETSI,[118] and IEEE[119] to develop industry standards. This includes development of common specifications, and certification to validate conformance of products and solutions prior to deployment by operators. Open interfaces are a key feature and principle of Open RAN development.

In interviews, stakeholders stated that uniformity and standardisation are important to success in open architectures, and this will lower entry barriers for smaller innovators. However, there are significant issues and details which need to be addressed to improve standardisation.[120] Stakeholders were keen to emphasise that standards should be open and global to enable

[113] https://web.archive.org/web/20140208025938/http:/www.4gamericas.org/index.cfm?fuseaction=page&sectionid=242

[114] https://www.etsi.org/technologies/nfv

[115] This view was expressed by a stakeholder in an interview for this project with Plum and Stratix.

[116] https://www.o-ran.org/specifications

[117] https://www.3gpp.org/news-events/3gpp-news/open-ran#:~:text=Open%20RAN%20is%20made%20possible%20through%20standardized%20open,architecture%20options%20and%20the%20associated%20open%20network%20interfaces.

[118] https://www.etsi.org/newsroom/press-releases/2120-2022-09-etsi-releases-first-o-ran-specification?highlight=WyJvcGVuIiwiJ29wZW4iLCInb3BlbiciLCJyYW4iLCJyYW4ncyIsIm9wZW4gcmFuIl0=

[119] https://standards.ieee.org/industry-connections/open-ran/

[120] These views were expressed by stakeholders in an interview for this project with Plum and Stratix.

innovation, and through coordination there is a need to avoid “balkanised” development of standards.

7.5 Security

The evolution of networks and provision of services creates cybersecurity risks which must be managed. The need for security of systems and data is technology neutral and must be maintained through each generation of technology change.

A number of dynamic factors affect cybersecurity risks. For example, the disaggregated software and vendor landscape in Open RAN networks creates challenges in the coordination of security activities, and shared infrastructure means that robust access control arrangements are needed to mitigate the risk of data leakage. ECN operators and their vendors must take care to ensure that their systems comply with security and data protections requirements which vary between jurisdictions.

Security and data protection challenges are a key consideration for ECN operators, and they have been a central feature in the planning and development of cloud-based solutions, softwarization and virtualization. Studies of 5G security risks have identified some risks associated with Open RAN, and also opportunities for security improvements from open and transparent interfaces. ECN operators take security very seriously and say they will not implement systems which are not secure and/or do not comply with the security and data protection requirements in each jurisdiction where they operate; equally, vendors know there will be no market for solutions which do not meet these requirements.[121]

7.6 Environmental sustainability

The move to more software based, virtualised and cloud-based ECNs is affecting the environmental impact of service provision. Network evolution involves more efficient storage and transmission of data and reductions in physical infrastructure. For example, cloudified data storage can reduce the need for bricks and mortar data centres.

Whilst physical infrastructure will remain a feature in ECNs, physical network footprints are to be reduced. This means reductions in energy consumption and fewer physical site visits. The environmental impact of cloudification, softwarization and virtualization is hence expected to be positive (if optimal conditions were to be implemented).

Nevertheless, our research and our discussions with different stakeholders have shown that whereas environmental issues and sustainability are core concerns shared by all of them, the positive relationship with networks and services cloudification is theoretical and too early to assess. Improving data collection and fostering the ability to make solid assessments of the

[121] In interviews for this project with Plum and Stratix, ECN providers and vendors reported that robust and compliant security and data protection capabilities are a minimum requirement for network and systems evolution.

environmental impacts of cloudification, softwarization and virtualization is still work in progress.

8. Impact of technical evolutions on market dynamics

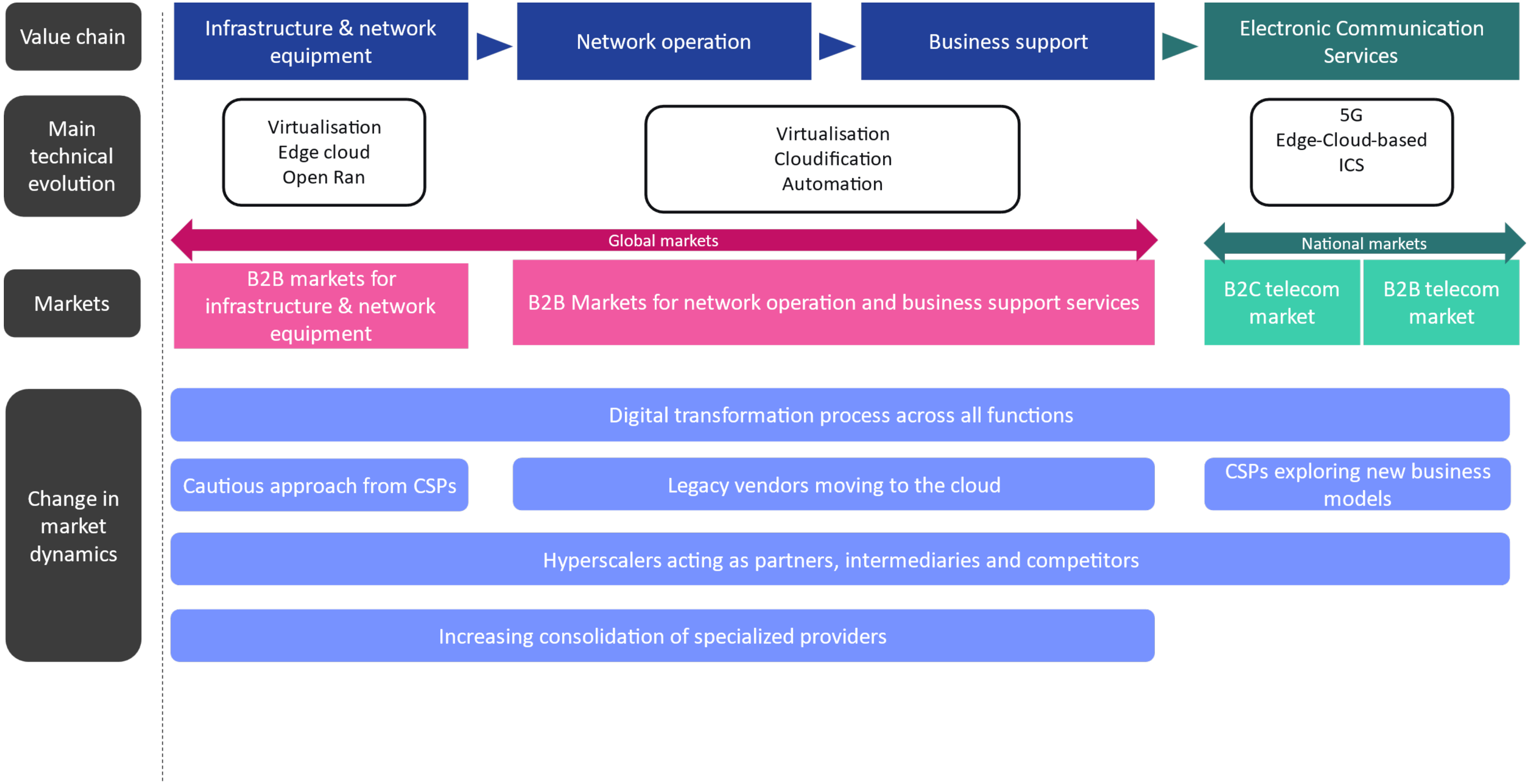
In this section we examine the impact of the technical evolutions described in this report on the dynamics of electronic communications markets. We consider the impacts and implications for CSPs, and on competition in these markets and markets upstream (e.g. network equipment markets).

We have identified a number of trends in market dynamics, and we describe these in this section. These trends sometimes directly affect the business models of CSPs providers, and sometimes also have a broader impact across the sector or between sectors. Generally speaking, these trends can be observed across different points in the value chain – in other words, they cannot be identified as relating directly only in one area (e.g. infrastructure and network equipment) and tend to have impacts across different value chain components. Therefore, in this section, we describe the impacts thematically by each of the trends we have identified, rather than dividing them by network and service components, following this structure:

- CSPs have embarked on a digital transformation driven by technical evolution;
- CSPs are adopting a cautious “wait and see” approach in some cases;
- CSPs are exploring new business models but face uncertainty;
- Hyperscalers have an increasing and multifaceted role; and
- Diversification, open systems and other competition implications.

These trends are also summarised in figure 8.1 below:

Figure 8.1: Trends in market dynamics related to cloudification of ECN/S



Value chain
Infrastructure & network equipment
Network operation
Business support
Electronic Communication Services
Main technical evolution
Virtualisation
Edge cloud
Open Ran
Virtualisation
Cloudification
Automation
5G
Edge-Cloud-based ICS
Global markets
National markets
Markets
B2B markets for infrastructure & network equipment
B2B Markets for network operation and business support services
B2C telecom market
B2B telecom market
Change in market dynamics
Digital transformation process across all functions
Cautious approach from CSPs
Legacy vendors moving to the cloud
CSPs exploring new business models
Hyperscalers acting as partners, intermediaries and competitors
Increasing consolidation of specialized providers

8.1 CSPs have embarked on a digital transformation driven by technical evolution

In the same way as other large companies, CSPs have embarked on a digital transformation journey to leverage technological advancement to modernise their operations and sometimes provide a better customer experience. A significant aspect of this transformation hinges on the efficient management of their networks which requires flexibility, scalability and cost-effectiveness. The use of cloud-based solutions across their operations is a key element of this digital transformation.

At the upstream level of the ECS value chain, the digital transformation involves the upgrade of network solutions as well as the deployment of new technologies and architectures. CSPs deploy advanced analytics and artificial intelligence across the different parts of the network. CSPs are shifting from a network architecture paradigm to a software development paradigm.[122]

This transformation differs between CSPs. For example, it is likely to be approached from a different starting point by operators deploying brownfield rather than greenfield solutions.

Transformation is more evident in network provision and management, and in support systems than in the consumer/end-user experience of ECS.[123]

The COVID-19 pandemic has also been a catalyst of this transformation, as the demand from end users for capacity and resilience have increased.

8.2 CSPs are adopting a cautious “wait and see” approach in some cases

In some areas, CSPs have adopted a more cautious approach to transformation. For example, the development of OpenRAN, described in Section 7.1, has seen a small number of deployments of greenfield networks, but so far a more cautious brownfield approach is followed by established networks through trials and more limited commercial deployment.

The cautious approach adopted by CSPs seems to be driven by a combination of technical, standardisation, financial and operational factors. These are discussed below:

- **Technical factors**: Virtualization of network functions introduce a level of complexity that CSPs need to carefully manage because of the mission-critical nature of telecom

[122] This trend was discussed and confirmed in interviews with stakeholders conducted by Plum and Stratix.
[123] This trend was discussed and confirmed in interviews with stakeholders conducted by Plum and Stratix.

networks. CSPs are cautious about implementing new technologies when they need to maintain network reliability and performance, and customer experience.

- **Standardisation factors**: Interoperability is a key issue as CSPs need to ensure that virtualized components from different vendors work seamlessly together and with existing hardware to avoid any service disruption. Some technology developments require extensive testing and the development of standardisation across interfaces before being suitable for wide adoption across networks.[124] Some disaggregated systems add complexity to integration, and this increases the need for testing and standardisation. Automated processes are helping this, but standards in some areas are still at an early stage of development, and some operators prefer to wait for clearer industry-wide standards before fully committing to transition their legacy infrastructure.

- **Financial factors**: While cloudification, softwarization and virtualization have the potential to reduce capital and operational expenditures in the long run, there are significant upfront costs associated with infrastructure upgrades and software development. CSPs need to assess the return on investment (ROI) and carefully plan their migration strategies.

- **Operational factors**: CSP's staff need to acquire new skills and expertise to manage virtualised networks. Training and upskilling staff to manage effectively can take time. In fact, several CSPs have expressed their concerns regarding the scarcity of relevant expertise within their teams.[125]

Therefore, technology evolution of CSPs does not necessarily provide a first-mover advantage. In fact, being a first mover in cloud adoption may not guarantee success, if a CSP fails to address other critical factors such as customer experience, service continuity, standardisation and security. This explains why the pace of transformation is uneven between CSPs, especially as it affects the riskier parts of the value chain. Whilst cloudification, virtualization and softwarization aims at driving operational efficiencies for CSPs, they have also contributed to a more complex vendor landscape which requires evolution in the approach to testing, integration and standardisation (as well as procurement).

[124] In interviews, stakeholders described to Plum and Stratix how test facilities are available for disaggregated OpenRAN components, and development of testing and standardisation frameworks is ongoing.

[125] This concern was discussed in interviews with stakeholders conducted by Plum and Stratix.

The emergence of new technologies and new players in the market has, in different ways, transformed the relationship between vendors and CSPs. CSPs that have internal resources to develop and operate their own software and IT stack[126] can become less reliant on traditional vendors and their solutions. For example, a major wholesale and B2B European telecom company that underwent a large-scale cloudification and virtualization of its networks has mentioned that the relationship with their legacy vendors has been “very complicated” during the transition phase, especially because the CSP has developed most of the software internally and has used its own private cloud. This has significantly changed the commercial relationship with its legacy vendors as it has reduced the need for their services over the past years.

On another note, disaggregation has brought complexity into the ecosystem but has also opened the way for more opportunities for CSPs. Nevertheless, these opportunities have yet to materialize as CSPs recognize the need for a “more agile and less siloed” working relationship. Besides, interoperability has been identified as a key barrier for the development of a multivendor procurement strategy and, as a consequence, sourcing a full system solution from a tier-1 vendor is still the preferred approach for some large European CSPs[127]. In terms of vertical relationship, this means that there is a potential way-out from a vendor lock-in situation, but interoperability and standardization are still key barriers.

[126] This trend was discussed and confirmed in interviews with stakeholders conducted by Plum and Stratix.
[127] This trend was discussed and confirmed in interviews with stakeholders conducted by Plum and Stratix.

Text box 8.1. Business models for cloud-based services

The technology developments which have characterized the evolution of electronic communications network functionality described in this report have given rise to a number of opportunities to provide cloud-based facilities and services in markets across multiple economic sectors. The emergence of companies providing virtual cloud based and softwarised solutions have facilitated business models which are becoming prevalent in multiple settings.

In many cases these compete with, or have replaced physical IT systems which were integrated within individual companies (typically located on their own premises). This evolution means that customers can opt to retain varying degrees of control over their IT functions (often a cost driven as well as operational decision for them).

Cloud-based business models

Infrastructure as a Service (IAAS)	Platform as a Service (PAAS)	Software as a Service (SAAS)
On demand infrastructure resources for compute, data storage and networking	Cloud services providing access to a virtual environment to develop, test and deploy applications	Complete applications hosted in the Cloud

These capabilities and services are relevant to our study because they can be deployed in ways which affect the provision of ECN/S, for example through telco cloud solutions. CSPs are often customers rather than providers of these services. A variety of companies are active in the provision of these services including hyperscalers which are significant in the ecosystem, providing services in each level of the cloud value chain.[128]

8.3 CSPs are exploring new business models but face uncertainty

8.3.1 CSPs diversify into new markets and services

CSPs business models have traditionally focussed on selling voice and data services over their own physical networks in a particular geographic area to generate revenue. Digitalisation has enabled the separation of the provision of services from the provision of networks. When the liberalisation of the telecom market started in the 1980s and 90s this was seen as a way to generate new revenue streams and provide services outside of the geographical coverage of the physical network. The result has proven to be far more dynamic. The technology

[128] See Ofcom's Cloud Services Market Study for analysis of this https://www.ofcom.org.uk/__data/assets/pdf_file/0025/244825/call-for-inputs-cloud-market-study.pdf

evolution described in this study has created risks to these perceived core revenue streams, but also opportunities for CSPs to diversify and build new business models.

CSPs have been able to build upon their strengths, leveraging their network infrastructure to provide connectivity between cloud facilities and between users and cloud facilities (sometimes called Network as a Service – NaaS).

There has also been a global trend of CSPs increasingly looking to shift from providing connectivity, voice and data into new value-added services to both individual consumers and businesses. Doing this involves three strategic and complementary approaches:

- Identifying new revenue streams
- Reducing costs
- Improving operational efficiency

All three approaches suggest that the traditional CSP's business model is evolving which inevitably has an impact on network operations and business support. According to a study by TM Forum, 72% of CSPs believe 5G revenue growth will depend on OSS and BSS transformation[129].

Additionally, solutions offered by vendors show that they are aligned with these approaches. For example, on efficiency and cost reduction, Nokia's digitalised network deployment service promises a 30% reduction in time-to-market compared to a traditional deployment approach. Rakuten's large-scale automation service up to 80% reduction in deployment time. Figure 2 contains some examples of new business models in development by CSPs.

Figure 8.2: New business models developed by CSPs[130]

CSP	New service
Batelco	Digital post box to enable secure communications between customers and public entities.[131]
Vodafone	Multi-cloud management and optimisation tools for business customers[132]

[129] https://www.tmforum.org/press-and-news/5g-revenue-growth-ossbss-transformation-press-release/

[130] https://www.novatiq.com/telco-business-models-changing-heres/#:~:text=For%20decades%2C%20the%20telco%20business,partnerships%2C%20and%20routes%20to%20market.

[131] https://batelco.com/business/the-first-digital-postbox-in-the-middle-east-launched-by-beyon-connect-in-bahrain/

[132] https://www.vodafone.co.uk/business/cloud-solutions/cloud-services

CSP	New service
KDDI	Digital advertising platform offering a privacy-safe end-to-end digital advertising solution in the Asian market[133].
Verizon	Advanced vehicle tracking system[134].

These diversifications by CSPs illustrate an effect of technology change and evolution on their strategy and business models. The new services, facilities and capabilities created by this type of diversification are not ECN/S and so, on their own, not subject to electronic communications regulation. However, they may fall within the scope of regulatory activity, for example, if they were bundled with regulated services. .

8.3.2 CSPs are also adapting their ECN/S business models

Section 5 of the report explains that because some players have entered the market and some have specialised in specific domains of the ECN/S value chain, both business models and relationships between market players and their suppliers have evolved. We have seen this in the diversification of the supply chain (and some of the standardisation, testing, and integration challenges which resulted from this).

CSPs have hence been able to adapt their operations and business models to leverage the benefits of availability of cloud facilities including IaaS, PaaS and SaaS. These transformations are evident in infrastructure and network equipment, network operations and business support as described in this report.

Cloudification, virtualization and softwarization are less easy to define in downstream consumer and end-user facing parts of the value chain, partly because of the diversity of end-users. Enterprise and business customers may be able to purchase bespoke cloud-based solutions as part of their communications services.[135] The impact of cloudification, virtualization and softwarization on the individual residential customer experience is currently less visible, but may become more so as technology evolution enables innovation in use case and service development.

[133] https://www.novatiq.com/kddi-supership-holdings-supership-launches-next-generation-digital-advertising-distribution-platform-utilising-novatiqs-technology/

[134] https://www.verizonconnect.com/uk/solutions/gps-fleet-tracking-software/?lead=Google%20Adwords&utm_source=google&utm_medium=cpc&utm_campaign=8968365261_UK_en_SPART_Brand_BR&utm_content=UK_en_SPART_Brand_BR_VerizonConnect_Non-DKI&utm_term=verizonconnectreveal&gclid=Cj0KCQiA6LyfBhC3ARIsAG4gkF9vQrDGsLaKGjkbj3IPy7hFCTL2337jBKSZrKLUsLjJmPrJflf06VMaAl4bEALw_wcB

[135] For example, cloud based private networking.

Text box 8.2. Factors affecting CSP cloudification business models

CSPs are not a monolithic category of players, nor are the business models within each of them. So cloudification related strategic choices will be affected, amongst other things, by whether a CSP (or a line of business within a CSP) is an incumbent or a challenger, a 'general purpose' MNO or a niche player MVNO, a B2C- or a B2B-service provider, a wholesaler or a retailer.

Whilst we have not identified conclusions which can be applied across all types of CSPs, we have observed some insights and trends, including:

- **Mobile vs. fixed CSPs**. Public sources on cloudification of ECN/S in the network tend to focus on mobile issues (Open RAN, core 5G) and rarely address cloudification of fixed and cable operators. Reasons cited for this include the timing of 5G transition, the complexity of RAN software, and current industry and academic interest in OpenRAN[136].

- **Divergent evolution**. With mobile networks, the focus is on introducing the next G, either by adding new spectrum bands, or by refarming existing bands. Fixed operators focus on phasing out copper, upgrading cable or building out FTTX. Per-country differences and legacy also play a larger role than with mobile. Relevant initiatives are taking place in fixed networks, and development of cloud and edge facilities to improve the delivery of data and customer experience in fixed network may be a further evolutionary step. It must be noted that greenfield mobile entry is very rare.

- **Size and revenue**. Smaller CSPs such as MVNOs and wholesale fixed-line operators are not in a position to make technology choices independently from their host network. Niche players such as ethnic or B2B brands manage their own BSS, not OSS. Lack of scale may limit investment.

- **Retail vs. wholesale**. Interviews have shown that wholesale providers as well as B2B operators are more advanced in their cloud migration compared to retail operators. This is mainly due to the different customer needs they have to meet. Large CSPs who operate retail as well as wholesale and B2B divisions seem to have a competitive advantage as experience with cloudification can be shared across the group, thus facilitating the transition for other subsidiaries.

- **B2B divisions** seem to have a competitive advantage as experience with cloudification can be shared across the group, thus facilitating the transition for other subsidiaries.

8.3.3 Challenges of evolution

The migration of networks and support solutions to the cloud is not an easy process because it means that CSPs need to move customised legacy applications to the cloud while maintaining a service continuity. Some operators have been able to successfully manage this

[136] This LinkedIn discussion on that matter includes ideas on the reasons behind this: https://www.linkedin.com/feed/update/urn:li:activity:7097306828945899521/

transition, using their own private cloud and in-house expertise. Leveraging internal capabilities is generally easier for large than small operators.

When the CSP relies on a third-party cloud provider, choosing the right solution is also not straightforward because of the technical complexity of the options and the large number of offerings available on the market. In fact, each operator has different requirements when it comes to the procurement of network operations and business support solutions and there is no unique buying-approach to these services. Some large telcos that run multiple carriers under one brand, such as Telefonica[137], GlobalConnet[138] or Etisalat seem to adopt an aggregated buying decision in order to standardise OSS/BSS platforms across each subsidiary.

Besides, the upgrade of OSS/BSS across markets for a large telco operating in different countries can also be a strategic step toward a new business model. Telia, for example operates in six countries and used to have six different orders to activation processes. It partnered with Ericsson to consolidate its OSS and BSS to the cloud and unified its product portfolio and processes across all six operating countries.[139]

Other operators, generally smaller ones, can mimic the buying decision of a larger competitor that went through a significant OSS/BSS upgrade and choose the same provider. This is known as the domino effect.[140]

8.4 The increasing and multifaceted role of hyperscalers

The role of hyperscalers in the cloudification and virtualization of the telecom value chain is multifaceted, with them positioning themselves as partners, intermediaries, and even competitors in the telecom space.

Hyperscalers have forged partnerships with traditional telecom software vendors to bring their services into the cloud environment.[141] For example, Amdocs, a leading software and services provider for communications, media, and entertainment industry sectors has partnered with major hyperscalers such as AWS, Google Cloud, and Microsoft. This partnership[142] means that Amdocs' services, such as billing, customer management, and operational support systems, can be hosted and scaled on these cloud platforms, offering flexibility, scalability, and cost efficiencies. Netcracker, another significant player in the OSS/BSS and orchestration

[137] Telephonica and Netcracker partnership: see https://passionateaboutoss.com/telefonica-uk-selects-netcracker/

[138] GlobalConnect and Comarch partnership: see https://www.comarch.fr/telecommunications/actualites/globalconnect-leader-nordique-de-linfrastructure-numerique-a-choisi-la-suite-comarch-pour-soutenir-son-offre-de-connectivite-croissante-geree-de-bout-en-bout/

[139] https://www.ericsson.com/en/blog/2022/6/bss-consolidation-takeaways-from-four-csps

[140] https://passionateaboutoss.com/aggregated-oss-buying-models/

[141] See for example AWS Local Zones which is discussed in Section 5.

[142] https://www.amdocs.com/sites/default/files/2023-02/amdocs-service-offering-review-2022.pdf

space has deployed its entire stack on Google Cloud[143] and Microsoft Azure.[144] This move does not only bring the benefits of cloud to Netcracker's offering but also taps into the global infrastructure and advanced services provided by these hyperscalers.

Additionally, hyperscalers provide platforms where specialized service providers can offer their telecom and IT services to a wider audience, thus acting as intermediaries between vendors and CSPs. AWS, for example offers a marketplace where OSS/BSS vendors can publish their offerings, and hyperscalers also provide services to facilitate linkages between CSPs and software developers. This PaaS approach benefits both telecom operators, who get a range of services from a single marketplace, and vendors like KloudGin and Flowmon, who can reach a broader audience without building their own distribution channels. This intermediary role has the potential to streamline the process for CSPs and fosters a community of solution providers.

Hyperscalers are not just limiting themselves to partnerships or intermediary roles; they're directly entering the telecom space, making them competitors to both CSPs and traditional vendors. Private networks, an area traditionally dominated by CSPs has seen the entry of players such as AWS. The hyperscaler offers private 5G services and provides a full suite of hardware and software solutions for private mobile networks.[145] A leading B2B European telco has also indicated that in the past year they have seen an increasing competitive pressure from Microsoft on the private networks market. In addition, hyperscalers are providing and working in satellite broadband connectivity,[146] and have invested in submarine cables.

Another layer of hyperscalers involvement in the telecom value chain is the direct investment in CSPs. Google for example, has invested $4.5 billion in Jio Platforms and indicates that hyperscalers see significant value in the telecom space, both as partners and stakeholders. Additionally, Amazon has also been considering a $2 billion stake in Bharti Airtel[147]. Such investments can influence the strategic direction of these telecom operators, further intertwining the worlds of cloud and telecom.

CSPs are still looking to build strong relationships with hyperscalers, although wary of the risk of dependency. For example, a CSP we have interviewed works with a hyperscaler in some areas of business development but does not want to have to fully rely on it, particularly for public networks and mainly because of privacy requirements.[148] More specifically, CSPs are looking for a homogeneous telco cloud, as standard, as open as possible (not vendor specific) and as commoditized as possible. Vodafone, for example, recently moved its RAN network data from multiple on-premises data lakes to one big “data ocean” on Google Cloud Platform.

[143] https://www.googlecloudpresscorner.com/2020-03-05-Netcracker-and-Google-Cloud-Announce-Strategic-Partnership-to-Help-Telcos-Modernize-Business-and-Operational-Systems

[144] https://www.netcracker.com/news/press-releases/netcracker-offers-ai-driven-digital-bss/oss-to-microsoft-azure.html

[145] https://aws.amazon.com/fr/private5g/

[146] For example https://www.aboutamazon.com/what-we-do/devices-services/project-kuiper

[147] https://techcrunch.com/2020/06/04/amazon-reportedly-considering-2-billion-stake-in-indian-telecom-operator-bharti-airtel/?guccounter=1

[148] Discussed in an interview conducted by Plum and Stratix for this project.

Once its data was collected into one place, Vodafone was able to quickly deploy an application, the Nokia Anomaly Detection Service, to identify and fix issues across the network.[149]

In conclusion, hyperscalers are becoming increasingly integrated with the telecom value chain. Their vast resources, technological expertise, and global infrastructure make them invaluable partners, while their ambitions and market strategies position them as formidable competitors. The line between telecom operators, software vendors, and hyperscalers is blurring, leading to a more interconnected, competitive, and dynamic industry landscape.

8.5 Diversification, open systems and other competition implications

The transformation and disaggregation of technical models through cloudification, virtualization, and softwarization in ECN/S market has had consequences for competition across the ECN/S value chain.

Disaggregation has created a more diverse and multi-layered supplier landscape and enhanced competitive dynamics. However, this has also resulted in some risks which are discussed in this report. In this section we look at the importance to competition of open systems and common standards, and describe the risks that, without these, new locked-in systems will emerge to the detriment of efficient competition.

8.5.1 The diversification of the cloud ecosystem

One consequence of the technical evolution identified in this study has been the diversification of the cloud ecosystem, with a variety of suppliers and vendors providing facilities and services to CSPs[150].

The landscape has become more complex with the entry of new market players. This has resulted in changes to the competitive landscape with new business models and suppliers emerging to offer solutions in the virtualised environment. For example, integration solutions to help CSPs manage the more complex disaggregated landscape of suppliers. Markets are dynamic, and with smaller suppliers entering the market to compete with traditional full integrated vendor solutions, one possible development is further consolidation and market concentration. This trend would build on some characteristics of the supply market (economies of scale, indirect network effects) and on the current “wait-and-see” approach from CSPs that has been identified.

[149] https://www.nokia.com/blog/see-how-saas-helps-csps-transform-their-business/)

[150] For the sake of a clear framework, and to avoid the classic chicken and egg issue between technology and business, our base assumption is that technology drives business as it has been presented in our technical proposal to BEREC, but we understand that this relationship is two-way and in some cases business ideas can be a catalyst for technological development.

Global and influential entities, many of whom are established in adjacent or related markets, have largely entered the cloud supply markets with ECN/S among their clients. Our study has identified that hyperscalers are active in various ways in the cloud value chain. Economies of scale and scope could enable them to become more influential in further market development and/or consolidation. Regulators and competition authorities have a legitimate interest in safeguarding competition in cloud markets, and hence are likely to remain vigilant to the possibility that dominant positions or concentrated oligopolies will emerge (see Section 9 for further discussion of regulatory implications). Cloud vendor lock-in becomes a potential concern, where migration from one cloud provider to another might prove challenging.[151]

The complexity of the landscape can be challenging; the lag between innovation and standardisation might pose interoperability challenges, and this risk is compounded when disaggregated functions mean there are more components and interfaces to manage.

8.5.2 The rise of open systems and the critical role of APIs in delivering good competition and consumer outcomes

The transition has also ushered in an era of more open systems, with APIs and their levels of openness playing a notable role in this evolution of the ECN/S value chain. Open systems are an enabler of positive competitive outcomes, and mitigate the risk of closed ecosystem lock-in.

API openness may have the positive impacts summarised here in Figure 8.3.

Figure 8.3:Advantages of open APIs

API characteristic	Impact
Open APIs	Open interfaces, especially in the realm of Open RAN, have allowed a multi-vendor environment. This leads to a more competitive landscape where proprietary systems are no longer the norm.
Interoperability	Open APIs promote interoperability among various equipment and solutions from different vendors. This means operators are not locked into a single vendor's ecosystem.
Faster innovation	Openness can lead to increased innovation as third-party developers and companies can introduce new features, applications, and solutions without waiting for the primary vendor to develop them.

[151] This is an aspect of the market identified and analysed by Ofcom in their work on cloud markets and reference to the Competition and Markets Authority. See https://www.ofcom.org.uk/news-centre/2023/ofcom-refers-uk-cloud-market-to-cma-for-investigation?utm_medium=email&utm_campaign=Ofcom%20refers%20UK%20cloud%20market%20to%20CMA%20for%20investigation&utm_content=Ofcom%20refers%20UK%20cloud%20market%20to%20CMA%20for%20investigation+CID_bd92b170f8b9abb05f9761e0b4673c25&utm_source=updates&utm_term=news%20centre

Cost efficiency	Operators have the freedom to select best-of-breed solutions rather than going for a complete package from one vendor, potentially leading to cost savings.
Automation and orchestration	With open APIs, it becomes easier to integrate various network operations tools. This makes automation and orchestration more efficient, resulting in faster service delivery and reduced operational costs.
Flexibility	Open APIs allow operators to make real-time modifications to their network operations without undergoing significant overhauls.
Multi-vendor management	With a diverse set of vendors of network equipment, managing operations can be challenging. Open APIs allow for the seamless integration of tools that can handle multi-vendor environments.
Enhanced monitoring	Open APIs allow for the easier integration of advanced monitoring tools, giving operators deeper insights into their network's performance.
Rapid service rollout	Open APIs allow for quick integration of new services and features into the existing BSS, enabling telecom operators to swiftly respond to market demands.
Enhanced customer experience	With API integration, BSS can offer more personalized services and recommendations based on real-time data analysis, improving customer experience and satisfaction.
Billing and revenue management	Open APIs make it easier to integrate various billing systems, enabling flexible billing structures and potential new revenue streams.
Third-party integration	Openness allows third-party service providers and vendors to integrate their solutions, leading to a richer set of services and capabilities offered to end customers.

In summary, API openness in the electronic communications sector introduces significant advantages across the value chain in cloudified and virtualised environments.

Open API solutions can of course also pose challenges – for example, ensuring security across open interfaces in a multi-vendor environment, ensuring that APIs are not commercially unfair between parties, and maintaining standardization. Therefore, whilst the benefits are manifold, they come with the necessity of implementing robust governance and management structures.

8.5.3 Technical barriers and their implications

While the multi-vendor ecosystem created by the market transformation described in this report may offer diversity, scalability, and versatility, it also brings forth challenges, particularly in control and testing. One of the most prominent challenges lies in ensuring that components from different vendors interact seamlessly. Interoperability – the ability for different systems and devices to work together in harmony – is important. But ensuring interoperability is not easy, especially when there is no single entity overseeing and coordinating the process.

New standards initiatives are emerging for multi-vendor disaggregated environments. For example:

- the O-RAN Alliance[152] which promotes open interfaces and ensure the interoperability of Radio Access Network (RAN) components from different vendors;
- The Sylva Project developing a framework for software and integration framework for cloud and edge use cases.[153]

Interoperability and standardisation are important to competition. A relevant risk is that a lack of openness and standardisation will foreclose market entry opportunities for smaller players and favour those who can provide multiple solutions within a locked ecosystem. Hence, technical barriers may disproportionately impact smaller competitors, potentially further boosting the influence of global players who can leverage their inherent competitive advantages.

In essence, the technical transformation in ECN/S, led predominantly by cloudification, is reshaping the industry. From the diversification of the cloud ecosystem to the emergence of new technical barriers, the implications are manifold and varied. How different segments of the industry respond to these challenges will shape the future of ECN/S market dynamics.

[152] https://www.o-ran.org/
[153] https://sylvaproject.org/

9. Discussion on potential challenges for regulation

To complete this study, we have assessed the implications of cloudification, virtualization and softwarization for regulation – in particular seeking to identify risks. This analysis and conclusions from it are presented in this section.

The study notes that deployment of cloudification, virtualization and softwarization in telecoms networks has been happening in some form throughout the 21st century. So it is not an entirely new phenomenon, though it has and will continue to evolve at fast pace. It is important then to recognise that, whilst this study is something of a "snapshot", regulatory analysis of these trends should be dynamic and ongoing.

It is helpful also to reflect on the scope of regulation because this does not always map neatly to the impacts of cloudification, virtualizatation and softwarization. The scope of telecoms regulation (in European terms ECN and ECS) is well defined in most jurisdictions, whereas the reach of cloudification, virtualization and softwarization as it affects CSPs activities is broad, crossing sectors and markets. This is evident in this study which, for example, identifies:

- ways in which CSPs are taking advantage of technology trends and opportunities to diversify away from their core business areas;
- that these trends have different effects when applied to operational and billing support system in comparison to their application in the operation of networks;
- changes in the vendor landscape; and
- the diversification of the cloud ecosystem, including increasing interaction between hyperscalers and CSPs which may affect regulated markets.

Regulators and policy makers will wish to continue to study the developments described in the report to identify their impact on regulated markets, and more broadly to consider the impact on policy and regulatory objectives.[154]

9.1. The evolving regulatory framework

The supply of ECN/S in Europe is regulated under a well-established system enshrined in the EECC. This system has evolved as markets have changed over the years,[155] and allows for

[154] For example the general objectives of the European Electronic Communications Code which are set out in Article 3 of the Code (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1547633333762&uri=CELEX%3A32018L1972)
[155] For example, accommodating the development of competition in retail ECS markets.

separate treatment of ECNs and the services delivered over them. Equivalent or similar provisions exist in other jurisdictions. The system provides effective safeguards to competition in the provision of ECN/S, and protects consumers against harm. It is a tried and tested framework which has been key to delivering effective competition and good consumer outcomes in Europe.

More recently, policy makers and legislators have developed new laws to meet the challenges of the digital society. Whilst digital services and content in scope of these laws are often delivered over ECNs and, in the case of cloudification, also support the provision of ECN/S, they are generally distinct from the provision of ECN/S and, as such, fall under different regulatory regimes. New legislation includes provisions to protect citizens from online harms, to promote effective competition in digital markets, to ensure fair access to, and use of, data, and to promote the interoperability and switching of data processing services. Examples of this in Europe are:

- The Digital Services Act providing protection from harmful content;
- the Digital Markets Act to protect a competitive level playing field in digital markets; and
- the Data Act, containing rules on fair access to and use of data as well as on interoperability, including for the provision of multicloud solutions, and switching of data processing services.

Whilst this evolution is relevant to consideration of cloudification, virtualization and softwarization in ECN/S markets, the new digital regulatory framework has broad applicability beyond the provision of ECN/S. Where digital regulation affects ECN/S, it is therefore appropriate for national regulatory authorities for electronic communications (NRAs) to liaise and collaborate with other authorities who are responsible for enforcing these statutes.

In the remainder of this section we examine areas we have identified which raise questions or challenges for regulation. This does not mean we have identified urgent cases for regulatory intervention; rather that we have studied consequences of cloudification, virtualization and softwarization which raise risks or questions relevant to regulated ECN/S markets. These can be studied and monitored further. In most cases the questions do not fall solely within the remit of NRAs, and so liaison and collaboration with other agencies and stakeholders is needed to progress work on them.

9.2. Regulation and competition

Cloudification, virtualization, and softwarization in the supply of ECN/S have contributed to improvements in ECS provision. For example, they have potential to:

- improve the efficiency of transmission and network management through virtualization and softwarization;
- enable providers to create scale in data storage through cloudification; and
- allow ECN/S providers to use common platforms for billing, service delivery and operational support provided and operated by third parties.

Improvements in the efficiency of service delivery has benefited consumers of ECS, for example because cost and scale efficiencies are delivered to consumers in the form of efficient prices and better operational performance in competitive markets.

Regulators will be concerned to ensure that these benefits are not diluted as a result of market failures. The European regulatory framework is well equipped to protect consumers from many types of market failure – for example, the EECC contains a well-established system for addressing competition issues and consumer harm arising from the existence of significant market power (SMP) in the supply of ECN/S.

However, more questions arise in relation to markets which fall outside of this system. We have identified questions in upstream markets for network equipment, where the number of suppliers has been reduced, and in related markets for digital services. We also discuss the risk that economies of scale in the trend to multinational and global solutions in virtualized networks may make it more difficult for smaller operators and smaller jurisdictions to develop bespoke solutions or forge bespoke vendor relationships for their markets and consumers.

9.2.1. Upstream markets and the vendor landscape

Our study has identified that cloudification, virtualization and softwarization has affected the competitive dynamics of some upstream ECS related markets.

These markets are not subject to specialist regulation, but the factors we have identified may have knock-on consequences in ECN/S markets. For example, the development of disaggregated models of provision for RAN components using software and functions from multiple vendors affect mobile access markets. We also found that some ECN/S providers are diversifying vendors and suppliers for core network equipment, BSS and OSS. This may have positive effects on competition and increased resilience.

The impetus to disaggregation has been driven in part by concerns about competition in the vendor market and the extent to which ECN/S providers face restricted options in their choice of vendor and/or the risk of lock-in to closed vendor systems. Disaggregation may therefore improve competition in vendor markets, and unlock innovation.

These changes to the vendor landscape are potentially significant for ECN/S provision - for example because they are creating a more diversified supply chain. This can deliver other benefits. Our analysis identifies that the disaggregation of network functions and diversity in the supply chain have the potential to strengthen the openness of systems (e.g. OpenRAN). However, this depends on a number of factors, including the transparency, availability and effectiveness of APIs linking systems and components, and the efficacy of standardisation and testing of new systems.

There is no evidence currently that these changes in the vendor landscape will lead to changes in competitive intensity between ECN/S providers. In interviews conducted for this study, some stakeholders speculated that the open interfaces and dissagregated functionality of OpenRAN may lead to opportunities for more differentiated propositions between providers which could strengthen competition. However others have mentioned that economies of scale, a lack of standardisation and testing and other factors, may also lead to market concentration.[156] It is also true that more or less competitive intensity in upstream suppy markets could lower or raise input costs which would in turn affect downstream pricing, including retail and end-user pricing. It is too early in the development cycle of vendor disaggregation to make robust forecasts on this.

Whilst electronic communications regulators do not regulate vendor markets, they have a direct interest in them as they are vital upstream inputs to ECN/S. Regulators will wish to continue to study and monitor the vendor landscape and, if necessary, take steps with other relevant authorities to ensure provision of ECN/S is not harmed by inefficient market concentration and the risk of vendor lock-in, and that open systems are efficient and secure. Since vendor markets are not subject to specialist regulation, this activity may require liaison and collaboration with technical standards bodies and cross-sector competition authorities.

9.2.2. Hyperscalers

In Section 8 we discussed the multifaceted role of hyperscalers in relation to ECN/S markets. The relationship between hyperscalers and ECN/S markets and providers is complex. It includes examples of hyperscalers as suppliers to CSPs, and situations in which hyperscalers are competitors to CSPs, both in the provision of regulated services and in other areas of CSP business. In Section 8, we reported that hyperscalers can deliver poweful benefits to the ECN/S value chain through their technological expertise, global infrastructure and financial strength. These can be delivered through their involvement in the ecosystem as suppliers, competitors or partners to CSPs.

There are also risks arising from the integration of hyperscalers with ECN/S ecosystems. Regulators and competition authorities are active in investigating these risks. For example:

[156] These points were raised and discussed in interviews with stakeholders.

- In 2022, the Dutch Authority for Consumers and Markets, ACM, published a market study into cloud services.[157]

- In 2022/3 the the French Competition Authority, Autorité de la Concurrence carried out an investigation of the cloud computing sector.[158]

- In 2023, following its own study the UK telecoms and media regulator referred the cloud computing sector to the Competition and Markets Authority (CMA) for investigation.[159]

- In 2022, the Japanese Fair Trade Commission reported on trading practices in the cloud services sector.[160]

The findings of these studies included some concerns, for example in relation to the propensity and ability of users to switch between cloud ecosystems, also addressed in the EU Data Act[161]. Whilst it should be noted that the analysis and findings in both these studies applied to the cloud market and were not focussed on ECN/S, electronic communications regulators will wish to monitor competition in the cloud market as it affects the communications sector. This may require liaison and collaboration with cross-sector competition authorities (for example, arrangements between Ofcom and the CMA in the UK, referenced above) and, in Europe, with the European Commission. Given the multilateral and global reach of cloud markets and companies operating within them, regulators may also benefit from liaison with counterparts in other jurisdictions.

9.2.3. Smaller operators and jurisdictions

One feature of ECN/S markets described in the report is the transition to virtualized environments in which network functions are abstracted from hardware. A consequence of this is that networks can share physical resources more effectively, and this in turn creates economies of scale in centralized platforms. Cloudification has added further economies of scope and scale.

These developments have delivered advantages to ECN/S providers in the form of unit cost reductions and more efficient provisioning of services. As noted above though, they have also contributed to markets in which vendors have sought scale to serve global markets, and cloud services markets are characterised by the prevalence of a small number of companies (with

[157] https://www.acm.nl/en/publications/market-study-cloud-services

[158] https://www.autoritedelaconcurrence.fr/en/press-release/cloud-computing-autorite-de-la-concurrence-issues-its-market-study-competition-cloud

[159] https://www.ofcom.org.uk/news-centre/2023/ofcom-refers-uk-cloud-market-to-cma-for-investigation

[160] https://www.jftc.go.jp/en/pressreleases/yearly-2022/June/220722_2EN.pdf

[161] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3491

some concerns expressed by regulators and competition authorities about barriers to switching).

In this environment, it has become more difficult for operators to seek bespoke solutions or features, for example which might be required to meet a regulatory requirement in the jurisdiction where they operate, or may be a service innovation and point of differentiation for them. This may be a natural consequence of the market operating efficiently at scale. However, generally operators have limited countervailing buyer power with some of the big equipment and cloud vendors and this is naturally more so in the case of smaller operators.

Evolution of the vendor landscape may address this issue to some extent because disaggregation could provide opportunities for innovation and market entry by smaller providers. However, as noted, the development of open disaggregated systems is at an early stage and outcomes cannot be predicted. Therefore, this can only be regarded as a potential mitigation rather than one which has crystalised.

As noted above, regulators will wish to continue to study and monitor the vendor landscape for any competition concerns which affect the provision of ECN/S. This will require liaison and collaboration with cross-sector authorities.

9.3. Efficient investment

A key objective of regulation is to facilitate connectivity and access to services for all citizens.[162] Whilst this is a widespread principle, its application can be very different between jurisdictions, depending on circumstances – for example, a country with a high penetration of PSTN may reflect this objective through an ambition to improve direct fibre connectivity, whereas as a developing country with poor fixed and mobile connectivity may do so by facilitating satellite connectivity.

Provision of connectivity requires significant capital investments. Like any capital intensive sector, electronic communications competes for capital with other sectors and projects in a global market. Requirements for investment in ECN/S provision and the availability of capital for this and other competing projects will be conditioned by the efficiency of the solutions provided. In other words, inefficient solutions will find it harder to attract capital.

Regulators have an interest in ensuring there are not barriers to efficient investment in connectivity and access. This may involve continued monitoring of the technology landscape and upcoming developments to ensure that this does not create risks. For example, in this study we identified that technology evolution creates the need for robust testing and sometimes standardisation work to deliver complex new systems.[163] Regulators should

[162] See for example, Article 3 of the EECC which includes the objective to "promote connectivity and access to, and take-up, of very high capacity networks, including fixed, mobile and wireless networks, by all citizens and businesses of the Union".

[163] For example, the GSMA initiative to align technical specifications for delivery of emergency calls over VoLTE https://www.gsma.com/services/blog/how-were-addressing-volte-emergency-call-issues/

continue to liaise with technical standards making bodies (where they are often observers) in order to contribute to the development of efficient solutions.

9.4. Access and take-up

The connectivity evolution we have described affecting the architecture and provisioning of networks and systems may lead to service and/or device innovation which directly affect the consumer experience and, potentially, the take-up of new services. There is a risk that innovation and development of new services delivers benefit to some users whilst others are excluded, for example because of the affordability of new services or devices. It is not evident that this is currently a consequence of cloudification, virtualization and softwarization in ECN/S value chains, but it could happen, for example if OpenRAN results in new use cases.[164]

This is a common feature of technology evolution, and is a reason why regulators have a role to facilitate universal service, promote digital skills and address barriers to digital engagement. Regulators have a role to study and monitor new services and devices to ensure end-users or groups of end-users are not excluded from participation and benefit.

9.5. Network and data security

Our study has identified network security considerations as a factor in cloudification, virtualization and softwarization. We identified that new technologies and network architectures affect the security of systems and data. Some stakeholders interviewed for the study mentioned concerns with regards to security, whilst others said that, because cloudification and virtualisation might put networks and services outside of the control of ECN/S providers, security checks and certifications have become more robust. Network operators and other stakeholders regard security as one of the most important requirements in migration to new technology systems which can create new risks, for example which result from open and more disaggregated architectures (as described in Section 6). Compliance with legal and regulatory requirements in this regard remains paramount in this environment.

Networks, vendors and regulators are working to mitigate incremental risks. A number of activities are in place for this. In Europe, the European Agency for Cybersecurity (ENISA) has an important role to develop cybersecurity capacity and address cybersecurity risks.[165] As described in Section 8, this includes work to identify and mitigate NFV related risks. The EU toolbox for 5G security is also an important facility to mitigate security risks.

[164] For example, in interviews conducted for this study, some stakeholders suggested that OpenRAN may create capabilities to create more bespoke services for each customer, potentially leaving less engaged consumers at a disadvantage.

[165] ENISA's remit is established under Regulation (EU) 2019/881 of the European Parliament and of the EU Council of 17 April 2019 (the Cybersecurity Act).

9.6. Environmental sustainability

In this study we report on the impact on environmental sustainability of cloudification, virtualization and softwarization. Some of this is positive relative to more traditional network architectures, including benefits from reduced use of physical hardware, reductions in site visits, and optimization of virtualized network functions. Nevertheless, there are also environmental costs, for example driven by the increasing need for data storage (even with more efficient solutions).

There are initiatives to reduce energy consumption and carbon emissions in the cloud ecosystem. Much of this is focussed on making data centres more efficient, both as an own initiative activity by operators and as a necessary step to achieve mandatory requirements. As noted, the Climate Neutral Data Centre Operator Pact seeks to achieve carbon neutrality by 2030.The Energy Efficiency Directive contains reporting obligations for data centres with a capacity over 500kW (including those of telecom operators) in the EU on their efficiency and requires data centres to meet certain efficiency targets by 2030. In some cases this will mean that data centres that can’t meet these obligations will be closed and the workloads will be moved to data centres (either private, colocation or cloud) that are in compliance with the directive. ETNO reported that their members have seen a decrease in scope 1 and 2 electricity consumption each year since 2018165. These reductions are across the entire business and not just related to the topics researched here.

Environmental sustainability is not typically a core responsibility of electronic communications regulators. Nevertheless, NRAs have undertaken studies of the environmental impact of the sector, the drivers of emissions and ways to address risks. It is evident that communications regulators and operators are increasingly mindful of and focussed on environmental outcomes, even where this is not at the centre of their remit. Areas in which NRAs are developing thinking on the environment include shared use of infrastructure and shared and coordinated responsibility for civil works (some elements of facilities sharing could be driven by technology evolution, for example, OpenRAN architecture may facilitate sharing opportunities). Whilst these areas are not all driven by cloudification, virtualization and softwarization, they demonstrate the importance of environmental sustainability in ECN/S and cloud ecosystems. It is expected that the focus on improving environmental outcomes will continue, and that NRAs will work with industry and other expert stakeholders on this.

9.7. Conclusions

Our analysis has identified a number of areas in which the technology evolution described in this report raises questions for regulators. We have not identified current market failures in the provision of ECN/S resulting from these developments, but there are a number of risks and areas for further study and monitoring.

The regulatory framework has also evolved to reflect the growing importance of digital services. Digital markets may affect (indeed are likely to affect) provision of ECN/S, but regulation of these cross-cutting areas is not solely the domain of electronic communications regulators, and hence continuing work, study and monitoring will require liaison and collaboration with other regulatory authorities.

In Figure 9.2 we summarise the areas which regulators may wish to continue to study and monitor.

Figure 9.2: Summary of regulatory challenges

Risk identified	Relevant statute/regulatory framework	Stakeholder authorities
Changes in upstream vendor and supply markets may impact ECN/S markets (e.g. through vendor lock-in and/or market consolidation)	EECC Competition Law	Electronic Communications Regulators Competition Authorities Standards Bodies
Competition in cloud markets, including lock-in and the influence of hyperscalers	Competition Law Data Act	Electronic Communications Regulators Competition Authorities (Other national competent authorities are designated for enforcement of the Data Act in each European Member State, however these entities are usually responsible for data protection, and not competition aspect of the Act)
Global vendor and cloud markets do not meet the bespoke needs of smaller operators and/or jurisdictions	Competition Law	Electronic Communications Regulators Competition Authorities
Ensuring technology evolution does not create risks for efficient investment	EECC	Electronic Communications Regulators Standards bodies
Ensuring citizens are not excluded from the benefits of technology development	EECC	Industry Electronic Communications Regulators

Protecting the security of networks and data	Cybersecurity Act Articles 40 and 41 of the EECC Directive on the Resilience of Critical Entities (as it relates to digital infrastructure)	Industry Electronic Communications Regulators ENISA
The need to reduce energy consumption and carbon emissions, and improve environmental outcomes	International treaty obligations (Paris Agreement) Elements of the EECC	Industry Electronic Communications Regulators Environmental agencies

As noted above, the trends analysed in this study are dynamic, and this study has been prepared based on the evidence available. Forecasting can be imprecise, and continued study and analysis by regulators is appropriate.

Appendix A: List of organisations interviewed

- AWS
- Cisco
- Colt
- Deutsche Telekom
- Ericsson
- European Advanced Network Testing Centre (EANTC)
- European Union Agency for Cybersecurity (ENISA)
- French Competition Authority (Autorité de la Concurrence)
- Google Cloud
- Juniper
- Mavenir
- Microsoft
- Nokia
- Open Fiber
- Orange
- Qualcomm
- Rakuten
- Telecom Italia
- Turkcell
- Vodafone
- 1&1

Appendix B: Interview questions

First round of interviews: Technical issues and market trends

1. Could you describe your firm, your position in the firm and what relations your firm has to NFV/SDN/OpenRAN/Cloudification?
2. What areas does your firm operate in with regards to these 4 developments?
    a. Are there specific areas your firm has a strong position in?
    b. Anything cool, interesting, extraordinary or a "first" your firm has in this field?
    c. Where does your firm distinguish itself from competitors?
3. Do you agree with the way we describe NFV/SDN/OpenRAN and Cloudification as separate but complementary developments? Is the separation in these four areas correct or do you see different developments that we should address?
    a. Are NFV and SDN really separate in your opinion or have they come together?
    b. Is it correct to use cloudification of the control of NFV/SDN/OpenRAN under the same header as cloudification of BSS/OSS or should we separate these?
    c. Are there other areas/terms that should be studied as part of this trend to virtualization and cloudification?
4. Do you think NFV/SDN/OpenRAN/Cloud deliver benefits to telecom operators and their customers?
5. How far towards maturity are NFV/SDN/OpenRAN/Cloud?
    a. Which ones are production ready in large telecom firms and which ones have promise for the future, but aren't production ready yet
    b. What can be improved in production ready technology?
    c. What is necessary to become production ready for other technologies?
6. What are the major benefits from the perspective of the telecom network/service operators' perspective to use NFV/SDN/OpenRAN/Cloud?
    a. Could you list some main benefits you see? (technical, financial aspects…) Any input about sustainability and cybersecurity?
    b. Which parts of the business will they be mostly visible?
    c. What type of customers of telecom firms will see these benefits translate in the service offers they get?
    d. What type of ROI do you expect for a typical operator? Can you put a number on it, e.g. as monetary value, percentage of Capex/Opex, per million customers?
    e. Are there examples of networks who quote these numbers as having been realised?
    f. How does this compare to more traditional set-ups?
7. Standardisation and flexibility are sometimes complementary, other times they affect each other negatively. For NFV/SDN/OpenRAN/Cloud, where in its business will the telecom firm see drawbacks as a result of the choices it has made? For example:
    a. Will it lose out on vendor specific innovation?

    b. Will it see more integration complexity?
    c. Will it be able to integrate a unique feature or regulatory requirement?
    d. Will it be able to differentiate its offer from other networks and service providers?
    e. Will the network be more intelligent or dumber? Is that good or bad?
    f. Will it affect interconnection?
8. How will NFV/SDN/OpenRAN/Cloud interact with service offers of MVNOs, both on the B2C and B2B side
    a. Will it become easier or harder?
    b. Will every telco become an MVNO in essence and the difference is primarily who bought the spectrum license?
9. How will NFV/SDN/OpenRAN/Cloud affect private LTE/5G markets?
10. How is the interaction between handsets/devices and the network under NFV/SDN/OpenRAN/Cloud? 4G and 5G voice (VoLTE) has proven to be harder to implement in a compatible way between devices and networks, how is this when NFV/SDN/OpenRAN/Cloud become part of the mix?
11. How do you see competition aspects between vendors in NFV/SDN/OpenRAN/Cloud stack[166]?
    a. Will we see more competition between vendors of hardware? Routers, switches, RAN?
    b. Will this create more competition for Ericsson, Huawei and Nokia? Who will become the new players?
    c. Will this create new monopolies or oligopolies (particularly because of API locking)? i.e., SoC, baseband, etc. or platform vendors (i.e., Windows was open to all hardware, but hardware vendors didn't release drivers for other platforms anymore, making Windows the default platform)
    d. Will it allow telecom firms to better compete, or will they become more uniform?
12. On the demand side, what dynamics of choices from users do you see between public cloud and private cloud (latency, security concerns, etc.)?
13. Will national regulators still be able to enforce requirements, when production, configuration, control etc will all be in the cloud and virtual?
    a. Experience with VoLTE shows that smaller MNOs can't get chipset vendors or platform vendors to adapt their products to national MNOs and requirements.
    b. What if essential features break, who can a regulator hold accountable?
    c. How to ensure national security?
    d. How can competition be enabled by these developments?
14. Is there any use case, paper, or report you would like to share with us, that could illustrate and/or be used as a source in the study?

[166] Difficulties in switching have been raised in OFCOM Services Market Study, 5 April 2023, https://www.ofcom.org.uk/news-centre/2023/ofcom-proposes-to-refer-uk-cloud-market-for-investigation

15. What important things have we missed and are important for our research?

Second round of interviews: Competition and regulatory challenges

Impact on competition between ECN/ECS providers

1. How have ECN/S providers adapted their business models or created new ones to accommodate cloudification, virtualization and softwarization

- in infrastructure and netw ork equipment – access (RAN), core network, backhaul?
- OSS and BSS?
- retail services (consumer and enterprise)?

2. What impact is there on competition between ECN/S providers?

3. Will providers have opportunities for greater innovation and/or differentiation of their offerings?

4. How does/will cloudification, virtualization and softwarization affect the consumer experience?

5. There are at least 400 OSS/BSS providers on the market so what is the usual procurement strategy for OSS/BSS and network operations solutions? What type of contracts are usually used? How operators choose their suppliers?

6. How difficult is the management of legacy applications and cloud-native applications for CSPs? Does this have an impact on how they serve end-customers?

Impact on competition between suppliers/vendors

7. How has the evolution of networks affected supplier and vendor markets

- in infrastructure and network equipment – access (RAN), core network, backhaul?
- OSS and BSS?

8. What does the disaggregation of RAN components mean for competition in mobile ecosystems? Does the added complexity of disaggregated systems mean that new market concentrations may emerge in integration of systems? Is it making standardisation more difficult?

9. In a relevant geographic market do CSPs opt for different providers?

10. All traditional OSS/BSS suppliers seem to have upgraded their portfolio to offer cloud-native solutions. How do they manage legacy solutions that are still being used by their clients? Is there an advantage for suppliers who don't have to deal with such clients?

11. Some players such as Amdocs, have grown through several acquisitions. Do you think that the market for OSS/BSS and network operations solutions is going to consolidate in the future?

Are there new regulatory challenges?

12. Are there potential competition concerns for regulators and competition authorities as a result of cloudification, virtualization and softwarization

- in the provision of ECN/S?
- upstream in supplier/vendor markets?
- If not now, might these emerge?

13. Does technology evolution make it more difficult for national regulators to make and enforce national rules, e.g. in small markets in cases where local requirements and features are not supported by global supply markets?

14. How should regulators and competition authorities approach technology and network evolution?

Other questions

15. What factors contribute to varying paces of development between different parts of the world/jurisdictions?

16. Is there anything you want to add?

Appendix C: Acronyms

3GPP – 3rd Generation Partnership Project

BBU – Baseband Unit

BSC – Base Station Controller

BSS – Business Support Systems

BTS – Base Transceiver Station

CAPEX – Capital Expenditures

CSP – Communications Service Provider

ECN/S – Electronic Communication Networks/Services

EECC – European Electronic Communications Code

GSM – Global System for Mobile communication

HLR – Home Location Register

ICS – Interpersonal Communications Service

MNO – Mobile Network Operator

MSC – Mobile Switching Center

NFV – Network Function Virtualization

NRA – National Regulatory Authority

OPEX – Operational Expenditure

OSS - Operations Support Systems

OTT – Over-The-Top

RAN – Radio Access Network

SDN – Software Defined Network

VLR - Visitor Location Register

WAN – Wide Area Network

Appendix D: Use case studies

In this section, we examine use cases which illustrate current deployment of cloudification, virtualization and softwarization in electronic communications.

In discussion and agreement with BEREC, we selected three use cases for this exercise:

- 5G private networks;
- mission critical mobile public voice services; and
- Mobile Virtual Network Operators (MVNOs).

These are all areas in which the evolution from established models to models employing cloudification, virtualization and softwarization are either nascent, or unproven, or both. We explore changes which have been made already, the potential for future evolution, and associated opportunities and risks.

D1. Private 5G networks

As digitalization increases in all industries and the public sector, companies and other organisations (e.g. government departments, NGOs) are increasingly reliant on connectivity, demanding more availability, reliability, quality and flexibility. To address their connectivity needs, they use private as well as public networks. The functions and use cases which need to be supported within private networks are diverse across organisations ranging from single premises organisations, through campus style installations with several buildings, to complex industrial settings like factories and ports which require sophisticated remote automated functionality.

In this use case study, we look at the development of private cellular networks developed and operated using 5G technology incorporating cloud-based capabilities, virtualization and softwarization. 5G solutions are potentially attractive to organisations with sophisticated needs and are thought to have potential in industrial settings.

Some organisations are deploying 5G private networks based on need for particular functionality, often low latency.[167] However, adoption of 5G private networks has so far been slower than some expected. This may be due to a number of factors, including cost of deployment, supply chain issues, and lack of 5G enabled devices. Evidence suggests that organisations are approaching transformation cautiously, including the deployment of pilot projects.[168]

[167] For example, Belfast Harbour (https://newsroom.bt.com/belfast-harbour-and-bt-to-build-the-uk-and-irelands-first-5g-private-network-for-ports/), John Deere (https://www.networkworld.com/article/3609841/john-deere-invests-500k-in-private-5g-licenses-to-support-more-flexible-factory-networks.html)

[168] https://www2.deloitte.com/us/en/insights/industry/technology/private-5g-network-growth.html

One difference between public and private cellular networks lies in who has access to the wireless spectrum, and who owns and operates the network's base stations and infrastructure. With public networks, a mobile network operator (MNO) owns and operates the spectrum and the network infrastructure. Private 5G networks may operate on licenced or unlicenced spectrum, and private networks may have some level of dedicated access to infrastructure and/or spectrum. This enables an organisation to control availability and quality of service and efficient transmission of data to edge devices which connect the organisation's infrastructure, sites, and employees. Having this degree of control can provide improved flexibility to meet traffic profiles that differ from those for which public networks are designed (e.g. serving industrial sites with more uplink transmission capacity).

There can be substantial variations within this model, e.g. in the extent of network infrastructure and spectrum owned and operated by an organisation.

Availability of and access to spectrum is also a variable affected by regulation which differs between jurisdictions. For example, Europe and the USA have followed different approaches to the availability of unlicenced spectrum, and on spectrum sharing, which has resulted in faster deployment of unlicenced spectrum in the USA.[169]

D.1.1 Description of traditional delivery models

Use of wireless technology for private networks did not start with 5G. LTE (4G) has been deployed in private network environments ("private LTE"), providing modern connectivity options to many organisations.

Organisations have been able to deploy wifi based private networks for many years. For wider area deployment, organisations can operate private networks using proprietary platforms such as LoRa[170] or Sigfox[171] which provide capabilities to create wide area networks (WANs) for communications and IoT applications. However, these technologies lack the bandwidth and flexibility of LTE and 5G systems.

D.1.2 Evolution of the delivery model

LTE and 5G technology have given organisations opportunities to deploy more flexible and scalable private network systems with the added potential of compatibility with public networks, and lower costs.

5G private networks can leverage the principles of cloudification to provide dedicated cellular connectivity and services to specific organizations or enterprises. Instead of relying on physical infrastructure deployed on-site, private 5G networks utilize virtualized network functions (VNFs) and software-defined networking (SDN) to deliver the necessary capabilities.

[169] See for example https://www.eetimes.eu/europe-struggling-to-share-spectrum/

[170] https://lora-alliance.org/about-lorawan/

[171] https://www.sigfox.com/

This allows for greater flexibility, scalability, and customization compared to traditional networks. Some key features of this evolution are:

- Virtualization: The virtualization of network functions, where the functions traditionally performed by dedicated hardware are implemented virtually using software. This enables greater flexibility and scalability as network functions can be dynamically allocated, adjusted, and orchestrated based on demand. For example, virtualized base stations (VBS) can be deployed as software running on shared infrastructure, eliminating the need for dedicated hardware.

- Centralization and orchestration: Cloudification enables the centralization of network management and orchestration functions. Network resources and services can be managed from a centralized cloud-based platform, providing centralized control and efficient resource allocation. This simplifies the management and maintenance of private networks and allows for more agile and dynamic network configurations.

- Network slicing: Cloudification enables network slicing, which is the creation of multiple virtual networks on a shared physical infrastructure. Private 5G networks can be divided into virtual network slices, each tailored to specific use cases or organizations, while sharing the underlying infrastructure efficiently. This can facilitate better resource utilization and isolation, ensuring dedicated connectivity and quality of service for different applications and tenants. In practice there may be limits on the number of network slices which can be deployed, and the extent to which the RAN can be disaggregated.

Figure 8.1: Summary of wireless private network types

Delivery model	Technology	Technology characteristics
Traditional	WiFi	Geographically limited Dedicated infrastructure Incompatible with public networks Lack of protection against interference
	Proprietary WAN	Dedicated infrastructure Capable of connecting remote facilities for IoT applications Incompatible with public networks Proprietary
5G	5G standard	High-capacity data transmission Can share infrastructure through network slicing Centralized network management and orchestration Virtualization and softwarization of network functions Flexible and scalable

D.1.3 Benefits and risks of evolution

Cloud based 5G private networks can deliver a number of benefits to organisations. These include:

- Flexibility and scalability: Cloudification enables rapid scaling of network resources based on demand, allowing private 5G networks to easily accommodate changing requirements and support new applications or services (subject to sufficient RAN resources being available).
- Agility and innovation: Cloudification provides a platform for rapid deployment and innovation, allowing organizations to quickly roll out new services, experiment with emerging technologies, and integrate with other cloud-based applications or services
- Cost optimization: By leveraging shared infrastructure and virtualization through techniques like network slicing, cloudification reduces the need for dedicated hardware, leading to cost savings in equipment procurement, maintenance, and operational expenses.
- Efficient resource utilization: Cloud-based network orchestration and network slicing enable organizations to optimize resource utilization by dynamically allocating resources between different virtual environments based on their specific needs.
- Potential for low latency use cases (when this capability becomes available in network and user equipment).
- Customisation of services and capabilities to bespoke customer needs.

There are also some risk areas to manage. For example:

- Deployment of wireless systems in a private environment provides the opportunity to operate on unlicenced spectrum.[172] This creates risks, including of interference and congestion.
- Network security: Cloudification introduces new security considerations, such as protecting data in transit and when it is stored, securing access to cloud resources, and implementing robust identity and access management mechanisms.
- Interoperability and standards: managing the need for interoperability and standardization of interfaces and protocols to enable seamless integration of different network functions and components from various vendors and avoid lock-in with one or a limited set of providers.

D.1.4 Conclusions

[172] https://ltemagazine.com/5g-private-networks-tsunami-approaching-with-the-cloudification-of-corporate-telecoms

The development of cloud native and cloudified 5G private networks can deliver benefits and has potential for organisations wishing to improve the flexibility, scalability and functionality of private networks. These networks can leverage modern technology and network management techniques to offer operational and cost efficiencies as well as delivering richer capabilities.

There are risks and challenges which organisations deploying 5G private networks and their suppliers must manage. Some of these risks are not unique to cloudified 5G private networks. For example, the use of unlicenced spectrum is also a feature of Wi-Fi networks. These risks can be mitigated through effective network management and security. Over the next few years there will be an expansion of spectrum supply for private networks for 5G. Such spectrum is already available in Norway, France, Germany, UK and there are plans to make it available in other EU countries.[173]

Overall, cloudified 5G private networks offer opportunities to organisations requiring high performance, flexible and scalable private network solutions. Adoption is currently slow with organisations taking a cautious approach which may accelerate as pilots are completed, solutions become more readily available and use cases crystalise.

D.2 Mission critical mobile public voice

Emergency services (police, ambulance, fire brigades and others) have very specific communication requirements. Voice communication is an essential part of their mission critical operations, and must be available at all times and circumstances, particularly in crisis situations that overwhelm the public networks.[174]

Until recently, public mobile operators were not able to meet the emergency services' specific needs (e.g. priority routing). Newer 3GPP standards include features to meet those needs, and cloudification makes it easier for operators to provide these features.

D.2.1 Description of the traditional delivery model

Traditionally, emergency services have deployed their own networks for voice communication because the public networks could not deliver the availability, coverage, and functionality they required. Until the year 2000, these networks were usually based on analogue technology, leading to inefficient use of spectrum. Starting from 1988, a few countries implemented digital networks based on the TETRAPOL system, and from 2000 onwards, most European countries replaced their analogue networks with digital networks based on the newer TETRA (Terrestrial Trunked Radio) standard[175].

[173] The European Commission has issued a mandate to CEPT on use of the 3.8-4.2 GHz band for local network area connectivity. See: Mandate_3_84_2GHz_5tdWtypEqdiGwgjS2YTken1pMgs_82230.pdf

[174] Under some disaster scenarios, specific measures may be used where existing infrastructure is damaged, e.g. deployment of portable base station equipment or mobile generators.

[175] Svrzić, Slađan. (2021). 25 years of the TETRA standard and technology for contemporary digital trunking systems of professional mobile radio communications. Vojnotehnicki glasnik. 69. 426-460. 10.5937/vojtehg69-29340.

Several attempts have been made to replace these dedicated networks with services from public mobile networks. A well-known example is the Emergency Services Network (ESN) in the UK, which was contracted in 2014 and planned to be available in 2017; its most recent planning update has moved this date to 2029[176].

One of the challenges faced by these initiatives is the tight integration within traditional mobile networks. These networks were designed and built to provide standardised voice services to mass markets, and adding the features required for the emergency services has proven to be complex.

Another challenge is the coverage requirement; attempts have been made to improve coverage through national roaming mechanisms, but again implementing these mechanisms for a limited customer group has been proven too complex and/or costly, particularly when these customers also want to have a guaranteed priority while roaming.

D.2.2 Evolution of the delivery model

The principles of cloudification, virtualization, and softwarization are now enabling mobile operators to provide sector-specific services, including features for the emergency services, without impacting their mass market business. Key to this is ensuring effective integration with comprehensive testing.

Moving functionality from hardware into software (softwarization and virtualization) provides for more flexible networks and for more loosely coupled architectures. This in turn enables the operator to add sector-specific functionality, or to expose interfaces which allow the emergency services themselves to create their own features.

Moving functionality from dedicated hardware into cloud-based computing (cloudification) also makes the operator networks more scalable and easier to manage, which allows the operator to provide a more diverse portfolio of sector-specific features. Given the scale and mission of these operators, they are likely to build their own cloud infrastructure rather than relying on public clouds; smaller mobile operators may decide to offload some (less critical) functionality into public clouds.

Cloudification enables the centralization of network management and orchestration functions and allows operators to expose some of these functions towards external parties. For instance, a customer may have access to real-time network monitoring, and to automated provisioning functions. It also lets them manage their own subscriptions directly, rather than depending on the operator's operational support systems (OSS) and processes.

Cloudification also enables network slicing, i.e. the creation of multiple virtual mobile networks on a shared physical infrastructure. By allocating a network slice to emergency services, these

https://www.researchgate.net/publication/350481005_25_years_of_the_TETRA_standard_and_technology_for_contemporary_digital_trunking_systems_of_professional_mobile_radio_communications

[176] https://techmonitor.ai/government-computing/esn-emergency-services-network-airwave-home-office

services can be given full control of their communication (within the agreed constraints), letting them manage their own quality of service (QoS) and priority schemes. Slicing also allows mobile operators to use designated Public Protection and Disaster Relief (PPDR) spectrum specifically for the emergency services[177], adding spectrum from other bands as needed.

As all these developments are relatively recent, compared to the life cycle of the networks used by emergency services, there are currently no emergency services having adopted this model for their operational voice communication. However, emergency services in several countries have started the procurement process for this type of service. One example is the Dutch Ministry of Justice and Security, who have already started using an "Over the Top" (OTT) service as a fallback communication option[178], and have now started procurement for a full-fledged critical communication service based on public mobile networks[179]. The project assumes an architecture where the emergency services will have a shared "MVNO" type core, connected to the mobile operator core. Such an architecture is hypothetically possible through the old delivery model, but much easier to establish using softwarization and cloudification.

D.2.3 Benefits and risks of evolution

By utilizing cloud technologies, telecom operators can provide improved mission critical services to the emergency services, through:

- Flexibility and scalability: Cloudification enables rapid scaling of network resources based on demand, allowing mobile networks to accommodate the rapidly changing requirements of the emergency services in terms of capacity and functionality.
- Cost optimization: By enabling mission critical voice communications on top of public mobile networks, cloudification allows the emergency services to either stop maintaining their existing private networks, or to create a hybrid architecture which combines public and private networks. In either case, this will lead to cost savings in terms of equipment procurement, maintenance, and operational expenses.
- Efficient resource utilization: Cloud-based orchestration and network slicing enable operators to dynamically allocate resources as needed to the emergency services, and to shift critical operational functions from the operators to the emergency services.
- Improved resilience, by allowing for more redundant hardware within the radio access network, and by enabling national roaming arrangements specifically for the emergency services.

[177] See https://www.ericsson.com/en/news/2023/5/band-68-spectrum-a-lifeline-for-public-safety-services-in-europe for an example

[178] Refer to https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2023/04/14/tk-reactie-op-diverse-vkc-verzoeken-in-relatie-tot-de-politie/tk-reactie-op-diverse-vkc-verzoeken-in-relatie-tot-de-politie.pdf (in Dutch)

[179] Refer to https://eu.eu-supply.com/app/rfq/publicpurchase_docs.asp?PID=348468&LID=409634 (in Dutch, registration required)

However, the shift also brings new risks:

- Softwarization and cloudification lead to more flexible architectures, but this also means that operators will introduce new features more often. System integration for the emergency services will be complex, and additional testing will be needed for each change within the public network. Due to this constantly changing environment, there is a significant risk that mission critical voice services will take much longer to implement than foreseen. Emergency services should therefore ensure that their existing infrastructure will continue to support them, while gradually building up the new environment[180].
- Emergency services will have to decide where to host the functionality they provide on top of the mobile networks – in the operator's cloud, in the public cloud, or in a private cloud. Each of these carries its own risks, in terms of security, privacy, and lock-in.
- Public networks offer a best-effort service, without the required service level agreements (SLAs) on parameters that are mission critical, such as higher redundancy, better coverage, or longer operation in case of a power outage. Even where operators have premium SLAs for their enterprise customers, these are usually not good enough for the emergency services. While cloudification enables the shift of emergency services towards public networks, MNOs may find it difficult to achieve the required service levels. In particular, the resilience against power outages required for these services may be complex and costly to achieve.

D.2.4 Technical considerations arising from evolution

While the basic functionality required for the emergency services has already been standardized within 3GPP (including mission critical push-to-talk and push-to-video), there are still various architecture options being explored. These will lead to new standardisation requests, defining new interfaces between the relevant building blocks.

Using public mobile networks for the emergency services will also require a new approach to security and privacy, as existing controls have traditionally been based on a physically separate network.

D.2.5 Conclusions

Cloudification, softwarization and virtualization will enable new service delivery models for the emergency services, allowing them to fulfil their specific requirements while benefiting from the flexibility of new cloud-based architectures and the cost efficiency created by using mass market networks.

[180] The Dutch project mentioned earlier has acknowledged this by defining multiple development "plateaus", with critical voice remaining on the current infrastructure until plateau 3 (four years after the initial setup).

D.3 Cloudification and MVNO

Mobile virtual network operators are providers of public telecommunications services over the networks of mobile network operators. By definition, an MVNO does not own or control the end-to-end value chain, but parts of it. MVNOs Europe states that MVNOs currently represent around 10% of SIM cards in the European Union. The term “virtual” refers to the fact that MVNOs do not control radio frequencies and related mobile physical infrastructure (antennas, base stations etc.). However, MVNOs do control the necessary hardware/software/resources to provide wireless/mobile services and may own other telecom infrastructures depending on the extent of their business model.[181]

D.3.1 Description of the traditional MVNO model

MVNOs can take different forms depending on the operational components they manage (e.g. telecom networks and interconnection resources), ranging from a “light‘ MVNO basically a simple branded reseller to a “heavy” or “full” MVNO that only lacks spectrum. In case of a full MVNO, the operator will have an E.212 IMSI-range and mobile numbers in accordance with a national number plan.

Some incumbent MNO's have secondary no-frills or niche brands that operate separately from the main provider. There are also large numbers of independent MVNO's that operate under their own brand and target different markets. Some MVNO's target price conscious customers, others target immigrant communities and others cater to specific business segments, such as the Internet of Things. Some MNOs operate specific business units for the Internet of Things services, for example Telenor Connexion, Vodafone IoT, Orange Business services.

D.3.2 Evolution of the MVNO model

The name already says that an MVNO is a virtual operator. As discussed, more and more virtualization is taking place in the networks of mobile operators. In earlier iterations of mobile networks, the distinction with an MNO may have been clearer than it is today.

Thus, the key trends in this report can enable an MVNO to better and sooner develop their proposition, with more flexibility, less legacy systems and with more choice in suppliers, that may come from outside the traditional telecom vendor group. It may also lead to lower costs and a reduced dependence on the hosting MNO.

The IoT businesses of the MNOs are increasingly organised as MVNOs within the business of the MNO. The customers who deploy IoT technology operate generally on a global scale. They also demand coverage and access to networks wherever the device is located. IoT customers also require broader insight into the functioning of the network than consumers. They want to know if a device is unreachable, whether that is a device issue or a local issue in the mobile network the device uses. This determines whether they need to send a mechanic to fix the device or whether they can wait a few hours and expect the device to become active

[181] MVNO Europe – Response to BoR (22) 88 (europa.eu), MVNO Europe – Response to BoR (22) 88 (europa.eu)

again. Given that the customers are global and that they need interactions with the networks of many MNOs, the service providers need to operate globally as well. The result is that increasingly the IoT supporting MVNOs are global players that can but don't have to be full MNOs. There are even examples where some IoT suppliers legally operate an MNO in a small country, so that legally they appear to be a roaming MNO.

D.3.3 Benefits and risks

The benefits of cloudification for an MVNO are:

- By means of cloudification, virtualization and softwarization in telecommunications, an MVNO can develop different flexible market proposals such as niche services for fixed-mobile converged communications or enterprise services that deeply integrate with machine-type communications or industrial automation. This is especially the case for industrial companies with a 'captive audience' in a certain industry vertical.
- In some cases, an 'asset heavy' MVNO or a company with an existing cloud platform and user base can acquire spectrum and become MNO. Rakuten in Japan and 1&1 in Germany are examples, but those examples are quite rare. Having a well-functioning cloud platform may make it easier to make the step from MVNO that is dependent on others to becoming an MNO with its own network.

A risk for MVNOs from cloudification is that:

- The advances and advantages of cloudification are also available to the MNO, reducing potential benefits. An MVNO may need to use a cloud platform that is more flexible and works with more MNOs to gain an advantage. However, the cloud platform providers it uses may also offer their services to MNOs, allowing them to make use of the same systems.
- An MVNO cannot control the radio resources or differentiate therein. An MVNO cannot adopt or launch new technology sooner than the MNO. This makes it more difficult to introduce benefits from cloudification before the MNO whose network is used. Nor will it be possible to use an air interface with more uplink capacity for video production, surveillance cameras or unmanned vehicles. Nor will it be possible to offer higher download speeds or a better coverage.

D.3.4 Conclusions

Cloudification, virtualization and softwarization can influence the MVNO market. They may help to reduce costs and differentiate in services and lower entrance barriers for new providers. It will not change the amount of control over that indispensable resource, radio waves.

Appendix E: Complementary recent sources of information on cloud markets

Besides sources of information mentioned in footnotes in this report, the following reports, although they do not apply specifically to the ECNB/S sector, are complementary readings to have a full picture of the cloud sector:

- Autorité de la Concurrence, France, Concurrence du secteur de l'informatique en nuage, 29 June 2023, https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/informatique-en-nuage-cloud-lautorite-de-la-concurrence-rend-son-avis-sur-le

- OFCOM, UK, Cloud services market study, 17 mai 2023, https://www.ofcom.org.uk/__data/assets/pdf_file/0029/256457/cloud-services-market-study-interim-report.pdf

- Authority for Consumers and Markets of Netherlands, Market study into cloud services, 5 September 2022, https://www.acm.nl/en/publications/market-study-cloud-services

- Japan Fair Trade Commission, Competition in cloud computing and other disruptive technologies: What's on the horizon?, 28 June 2022, https://www.jftc.go.jp/en/pressreleases/yearly-2022/June/220628.html

- Webinar (in English) : Competition in the cloud sector, French, Dutch and Japanese Competition Authorities, https://www.autoritedelaconcurrence.fr/fr/article/evenement-echelle-mardi-3-octobre