Deployment models for telco cloud

Technical and policy perspective

White Paper

Document properties

Document title	**Deployment models for telco cloud - Technical and policy perspective**
Authors	**Olga Batura, Pieter Nooren, Prachi Sachdeva, Bastiaan Wissingh**
Reviewers	**Borgert van der Kluit, Sander van der Zande**
Dissemination level	**Public**
Status of the document	**Final**
Version	**1.0**
Work Package	**WP4.5 Technology-Policy Co-Development**
Deliverable	**Part of FNS Milestone M4.5.1**
Contractual delivery date	**December 2025**
Delivery date	**10 December 2025**
File name	**FNS6G_20251210_Deployment_models_for_telco_cloud_v1.0**

Major contributions to impact pathways

Sustainable earning power	
Digital autonomy and reliability	X
Sustainability	

Summary

Most Mobile Network Operators (MNOs) today rely on cloud services for essential IT systems, such as customer relationship management. Since the introduction of 5G, they also rely on so-called telco cloud systems to run their 5G core network. The fact that many cloud services are supplied by a relatively small number of non-European companies could raise competition concerns, security risks and issues of digital autonomy. Having these concerns in mind and looking towards the development of 6G, this white paper addresses two mutually related research questions:

- What are the cloud stack deployment models encountered in 5G mobile networks today and which roles and types of providers are involved?
- How do the cloud stack deployment models relate to European policies, including the Digital Markets Act, Data Act and NIS-2 Directive?

The white paper introduces the reader to the different layers of the telco cloud stack and related, commonly used terminology. It then presents the current deployment models of the telco cloud stack from two different perspectives as seen by the MNO: the supply chain perspective and the operational perspective. The supply chain perspective shows the various ways in which a cloud stack could be built up by the MNO using a combination of different types of suppliers. Each supply model is then broken down into the various operational view variants indicating which party would be in operational control of the different layers of the stack. The two perspectives of deployment models illustrate the dependencies the MNO experience in supply and operation of their cloud stacks.

Policy documents have repeatedly identified problems caused by the dependences of European companies on non-European cloud providers. This white paper analyses whether and how the current legislative framework (e.g. Digital Markets Act, Data Act and cybersecurity measures) addresses potential problems related to competition, security and digital autonomy, specifically in application to the telco cloud.

The paper concludes that, in practice, MNOs use a combination of different deployment models within their network and move between different cloud stacks because of the well-established Kubernetes Container-as-a-Service layer between the Cloud-Native Network Functions (CNFs) and the supporting cloud stack. At the moment, MNOs in the Netherlands do not use SaaS offerings, which is different from other sectors and application areas, like office productivity software, where SaaS offerings are very common. Additionally, so far, there is no use of public cloud services for the CNFs in the Dutch mobile operator core networks.

The white paper also finds that the EU-level legal instruments aimed at market regulation and increasing competition are unlikely to make a difference for the telco cloud. With regard to digital autonomy, there are no dedicated legal instruments at the EU level. However, cybersecurity legislation, the NIS-2 Directive and the EU Toolbox for 5G Security recognise some of the digital autonomy risks and offer recommendations for their mitigation. The paper finds that all analysed legal instruments look at cloud computing more generally and are not specific to the telco cloud. Additionally, the analysed legal instruments focus on the supply chain rather than operational control of cloud, whereas our research demonstrates that, in the telecom context, both are important and can result in competition or autonomy shortcomings.

In the further evolution of 5G networks and in 6G mobile networks, cloud will be used wider than just in the core section of the network and will also see different forms of deployment. This means that the importance of cloud stacks will grow further and could see new challenges. This will be investigated further in another FNS deliverable following up on this white paper.

Table of contents

1. Introduction

1.1. Mobile networks and cloud

Businesses and organisations, including government bodies, make extensive use of cloud services for their day-to-day operations. This is also true for the mobile network industry. Cloud technology and services can provide elasticity to meet growing demands of mobile network operators (MNOs). Many essential IT systems within MNOs, such as the Customer Relationship Management systems (CRM) can run on cloud services. These kinds of cloud services are often called IT cloud, and that is how we will refer to them in this document [1].

The focus of this document is on the so-called telco cloud rather than IT cloud. When the core network or the radio network of a mobile network is hosted on the cloud, it is called telco cloud. So far, MNOs tend to distinguish telco cloud from IT cloud because it typically has more stringent performance and QoS requirements. Both the telco cloud and IT cloud use the same architectural framework and agile principles for scalability. However, it is good to note that the radio network is geographically distributed based on the areas it serves. Some services and functions require extremely low latency and thus near real-time coordination. As a result, these functions cannot be installed on a central cloud, but require a distributed (or edge) cloud to run on.

The models presented in later chapters are focused on the core network part of the telco cloud. This white paper focusses at the models for cloud deployment, in so-called cloud stacks, for 5G networking. It will be followed up by another paper, which will discuss the evolution of the telco cloud in 6G.

1.2. Policy perspective on cloud

For a large part, cloud services as we know them today have been developed and marketed by well-known American companies such as Google, Microsoft and Amazon Web Services (AWS), and a range of comparatively smaller companies that entered this market as well. The technical and business models for cloud, and the structures of cloud stacks, are firmly established and at the same time constantly evolving. The services they provide are an integral part of the day-to-day operations for most companies.

While these business models work well for most users, there are concerns about over-reliance on a limited number of large providers [2], [3], [4]. It may lead to competition problems, such as lock-ins and bottlenecks to switching between cloud providers, and lack of interoperability between clouds, including for their parallel use. The prevalence of third-country cloud providers may cause security and digital autonomy concerns [5].

Digital autonomy is a broad concept without an agreed definition, but, at the heart, it means a country's or a region's ability to control its data, software and hardware that drive its digital systems. The Netherlands uses the term "digital open strategic autonomy" meaning "the EU's ability, as a global player, to safeguard public interests and be resilient in an interconnected world, in cooperation with international partners and based on its own insights and choices" [6]. In its agenda on the Digital Open Strategic Autonomy, The Netherlands has determined ten specific priority areas,[1] including network technologies and cloud, where there are risks of strategic dependencies. The government actions in these priority areas must contribute to 1) strengthening the European political and economic foundation, 2) mitigating risky strategic dependencies, or 3) increasing Europe's geopolitical capacity for action [6].

[1] These are 1) critical raw materials, 2) quantum technology, 3) photonics, 4) semiconductors, 5) network technology, 6) open source software, 7) cloud, 8) AI, 9) cybersecurity, and 10) office software.

1.3. Research questions

This white paper addresses two, mutually related, research questions:

- What are the cloud stack deployments encountered in 5G mobile networks today and which roles and types of providers are involved?
- How do the cloud stack deployments relate to European policies, including the Digital Markets Act, Data Act and NIS-2 Directive?

1.4. Future Network Services

This white paper has been developed in the Future Network Services (FNS) programme, the Dutch multi-year public-private program on 6G development. FNS works on specific and connected topics in 6G: intelligent radio components and antennas, intelligent networks, and leading applications in key sectors. This is combined with work aimed at strengthening the 6G ecosystem through a large-scale national 6G testbed and standardisation. Although FNS is a Dutch 6G programme, it is firmly embedded in the larger European and international effort on 6G development.

For the successful uptake of the technology, it is important that its development is well aligned with existing and future policies. This is the motivation for including research on policy-technology co-development in the FNS work on the 6G ecosystem, with cloud as one of the key topics. For the creation of new economic earning power in The Netherlands around 6G and to preserve the technological sovereignty of Europe, having autonomy over one's cloud systems is emerging as a priority. Last year the European Commission published a White Paper "How to master Europe's digital infrastructure needs?" [7], which examined the trends and challenges in the digital infrastructure sector and presented the concept of the Connected Collaborative Computing or the 3C network. This momentum also calls for a closer examination of the existing policy on cloud and how upcoming technology development would align with that.

The FNS partners contributing to the policy-technology work are (in alphabetical order): the Dutch Authority for Digital Infrastructure (RDI), Ericsson, KPN, Liberty Global, Ministry of Economic Affairs, Nokia, Odido and TNO. The role of FNS as a research and innovation project is to provide analysis and inputs for policy makers at the Dutch and EU levels. FNS does not have a role in policy decisions themselves.

1.5. Approach

The work presented in this white paper is a consolidation of desk research conducted on the current state of developments in the Cloud domain and the existing policies, as well as a study of the future trends. Further, interviews were conducted with FNS partners involved in the Policy-Technology work to gather the perspectives of the different stakeholders, such as government, telecom operators, and vendors. The following parties within FNS were interviewed: KPN, Odido, Nokia, Ericsson, EZ, and RDI. Additionally, relevant experts outside of FNS also provided input, such as those working on open cloud initiatives within Europe. Lastly, experts within TNO were also consulted. Overall, efforts have been made to ensure that a holistic view of the topic and perceived challenges for the future could be created. Finally, this white paper has also been reviewed by the FNS partners involved.

2. The adaptation of cloud in mobile networks

2.1. Adoption of cloud in 5G mobile networks

The evolution of the mobile network from 4G to 5G saw the integration of the cloud into communications networks in a major way. While 4G incorporated the Evolved Packet Core (EPC), 5G's core used a cloud-native Service-Based Architecture (SBA) that leveraged Network Function Virtualization (NFV) and Software-Defined Networking (SDN). The new 5G architecture [8] offered the ability to dynamically scale up based on the load and demand, a feature that was not present in 4G. At the heart of the cloud-native 5G was the shift from a single monolithic architecture towards a microservices architecture. Each microservice is a self-contained unit of code, packaged into a container, that is loosely coupled with the rest of the microservices, but runs independently. These could be core network functions like the Access and Mobility Management function (AMF) or the Session Management Function (SMF), or any of the other functions in a mobile network. One of the benefits of containerisation is that when one container is down, it only affects the function that it runs, and not the other functions. This is also what makes the 5G architecture more fault tolerant. However, it is important to mention that the 5G service-based architecture is highly interconnected in general. Of course, the use of the containers increases the complexity of the deployment as well as management. In order to manage these containers and provide services, orchestration is needed. This is usually done through an orchestration software like Kubernetes which is deployed within a cloud environment.

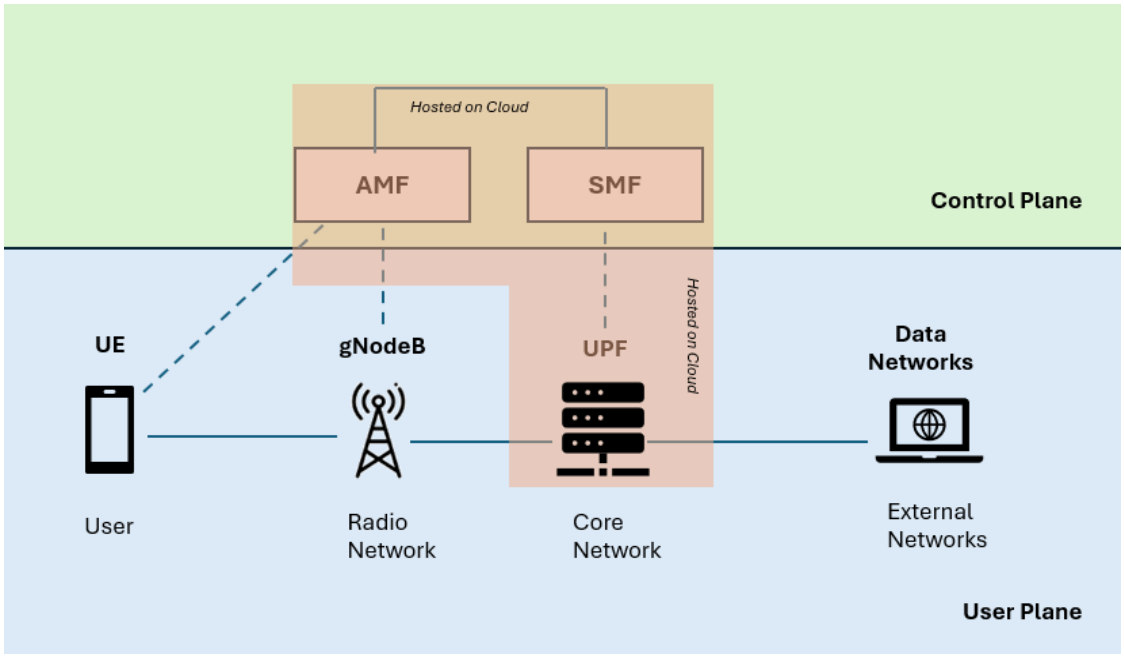

Figure 1: Simplified architecture of a 5G Network

In the figure, we see a simplified view of the architecture of a 5G network. The User Equipment (UE) connects wirelessly to the radio network of the operator, which has been depicted by a gNodeB, the 5G base station. This in turn connects to the core network with the User Plane Function (UPF). The UPF is a key component of the 5G core network that handles forwarding and routing of user data traffic. Within the core network, there are several other functions. For the sake of simplicity, this figure depicts only two of those, the AMF and the SMF. The AMF handles user connection, registration and mobility management, while the SMF is responsible for managing user sessions. The core network including the UPF, SMF, and AMF may be hosted on the cloud. Finally, the core network connects to external networks, like the public

internet. The figure above has also been divided into two sections – the user plane and the control plane. This is a logical separation in a mobile network, whereby the user plane carries user data like voice and video, whereas the control plane carries signalling traffic.

5G also focused heavily on edge computing, a concept where the processing tasks of applications are moved closer to the user, typically to reduce latency and the traffic load across the network. This allows support for time sensitive services, such as AR/VR, industrial automation, etc. This also gave birth to the term "cloud-edge continuum", which essentially is a computing model where computing resources are available from the central cloud data centres to the edge of the network, essentially distributing processing over multiple nodes and reducing latency.

2.2. The layered structure of cloud

Telco cloud networks are built of various layers which are stacked on top of each other. Each layer logically represents a service that could be provided by a single service provider. Thus, each layer in a stack could theoretically be provided by different providers, or all the layers could be with the same provider. This is what we explore further in Chapter 3. The figure on the left shows the various layers in a cloud stack. While the lowest layers of the stack still refer to hardware such as data centres which provide rackspace, power, and cooling, the topmost layers of the stack are purely software.

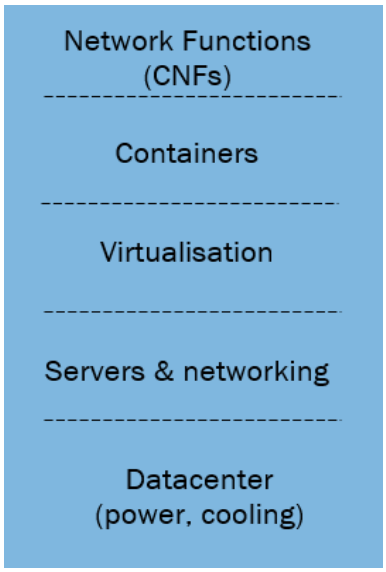

Figure 2: Layers of a cloud stack

At the top two layers in the stack, Cloud-Native Network Functions (CNFs) can be run on the containers in the layer underneath, on the virtualization layer or directly on bare-metal servers. A CNF is essentially software that replaces specialised hardware, examples are the AMF and SMF mentioned earlier. CNFs are packaged into containers, which also means they can be moved from one underlying cloud infrastructure to another, a concept called portability. Additionally, some telcos may also choose to deploy their CNFs on two or more clouds, essentially creating a multi-cloud environment that reduces the effects of vendor lock-ins, using a concept called interoperability (Section 3.2.1.8). Lastly, using multiple cloud environments that are interoperable and can share resources seamlessly is known as cloud federation [9]. Cloud federation helps organisations to leverage the strengths of multiple cloud service providers, and it also serves as a resilience measure in case one of the cloud providers is experiencing failures.

3. Cloud stack evolution to 6G

This chapter explores the various cloud stack models that are currently encountered in 5G networks and are also expected to be relevant for 6G. It discusses which providers play a role at which layers. However, when taking a closer look at the stacks, it becomes apparent that there are two perspectives. The first perspective is from the providers that supply the hardware and software components in each layer, while the second perspective is from the providers that operate the components. While this may seem unimportant at first glance, it has a profound relevance. While it is obvious that the supplier of a service exerts decisive control over the provision of the components, the one operating a network controls it in real-time and is responsible for the overall health and maintenance of the network. Both perspectives (the supply chain view and the operational control view) have a clear relation with digital autonomy. In the end, the mobile operator providing the 5G and 6G services is responsible, but it is important to peel down the dependencies that are created by the supply and operating models that mobile operators can choose from.

3.1. Commonly used terminology

Cloud computing can be provided as a combination of different deployment and service models. Deployment models describe where cloud functionality is hosted and by whom, while service models describe which cloud functionality is hosted by whom. In the applicability of these models, we specifically look at the case of deploying CNFs on cloud infrastructure.

Looking at the cloud deployment models, there currently exist three common models [10], [11]:

- **Private cloud**, where cloud resources are dedicated to a single organization and, hence, not publicly available. This does not necessarily mean that a private cloud is hosted on-premises, it could also be hosted in a private part at the premises of a cloud service provider.
- **Public cloud**, where cloud resources owned and operated by cloud providers are available to, and shared by, everyone over public internet or a direct connection.
- **Hybrid cloud**, a combination of public and private cloud environments. Here, typically, an organisation hosts its own private cloud, either within its premises or off premises, for a part of its data and connects it to a public cloud where another part of its data is hosted.

Section 2.2 above discussed the different layers that form the cloud stack. Corresponding to the layers, there are several services that are also possible in the cloud stack, depending on where in the stack they sit. Figure 3 below shows the cloud stack layers with the corresponding services added.

Regarding service models, the most common service models (bottom-up) in the industry are [12], [13]:

- **Infrastructure as a Service (IaaS)**, this service model delivers on-demand infrastructure resources to customers via the cloud, such as compute, storage, networking, and virtualization. Customers still need to maintain their own operating systems, middleware, virtual machines, apps and data.

- **Container as a Service (CaaS)**, this service model delivers and manages all the hardware and software resources that are needed to develop and deploy applications using containers. So, the environment to build and deploy containerized applications is managed and maintained by the cloud service provider while the customers still need to develop/ maintain their own code/ apps and data.

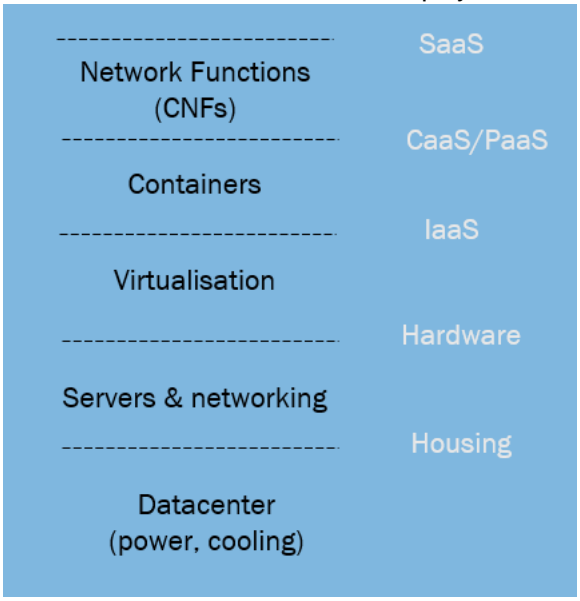

Figure 3: Cloud stack layers and corresponding services

- **Platform as a Service (PaaS)**, this service model delivers and manages all the hardware and software resources to develop applications through the cloud platform. So, the environment to build and deploy applications is managed and maintained by the cloud service provider while the customers still need to develop/maintain their own code/applications and data.
- **Software as a Service (SaaS)**, this service model provides the entire application stack, delivering an entire cloud-based application that customers can access and use. SaaS products are completely managed by the service provider and come ready to use, including all updates, bug fixes, and overall maintenance.

3.2. Cloud Stack Models

With the above-described deployment and service models as a basis, a series of interviews with Dutch telecom operators and European mobile network vendors have been conducted to create an overview of most used supply models and the associated operational models.

The different deployment models (*private/public/hybrid*) are depicted in the *Housing* layer, e.g. whether the solution is hosted by a mobile operator or cloud service provider. The different service models are depicted in the layers on top (*Hardware/IaaS/CaaS/PaaS*). While the *SaaS* layer of the service models is shown in Figure 3, it is not a part of the cloud stack models discussed in this Section. This is because it has not been encountered during the conducted interviews. As will be seen later, it is relevant when considering the future evolution scenarios for 6G cloud deployment.

Within the models, the following main types of providers/organisations are involved:

- Mobile operator: This refers to MNOs such as KPN, VodafoneZiggo, Odido, Orange or Telefonica;
- Mobile network vendor: This refers to companies like Nokia and Ericsson;
- Cloud service providers: This includes companies like Amazon, Microsoft, OVHcloud or Ionos;
- Middleware vendors: This refers to companies like VMware by Broadcom or Red Hat.

The next Section introduces seven different models for the supply chain perspective, and the subsections will address their respective model in detail. In Section 3.2.2, each model of the supply chain perspective is then broken down into the equivalent models from the operational perspective.

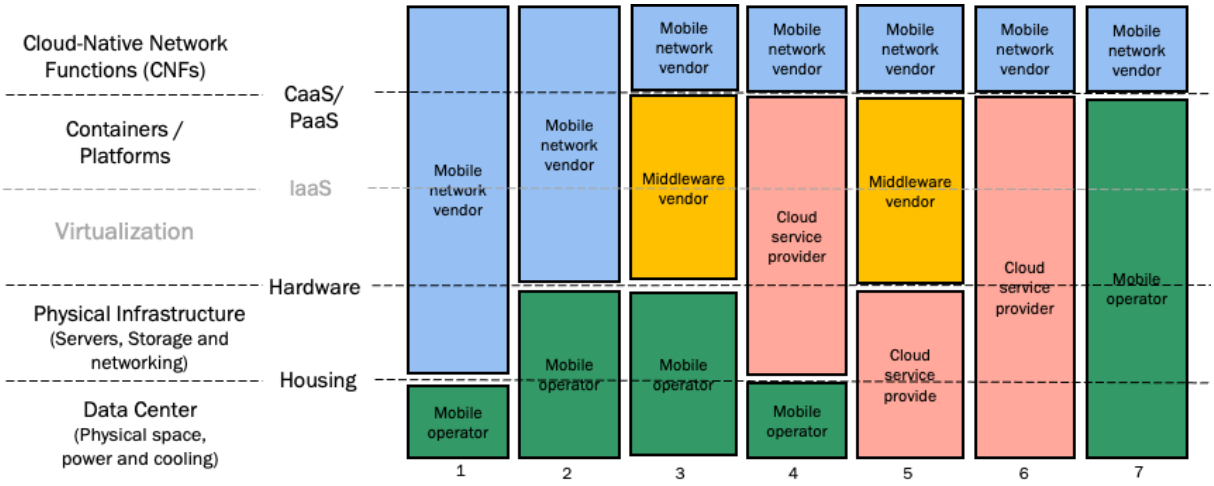

Figure 4: Cloud stack models from the supply chain perspective.

3.2.1. Supply chain perspective

The stacks presented in Figure 4 have been constructed from the MNO's point of view. The MNO needs a cloud stack in order to provide 5G/6G services to his customers. For each stack layer, the MNO has several options in vendors and service providers. However, the MNO may also choose to build parts of the stack itself, typically by integrating COTS (Commercial off the Shelf) hardware and software components in-house. In the case where the MNO decides to do so (i.e., self-supply), the corresponding layer of the stack indicates Mobile operator. When the MNO buys the services of the stack layer from an external organisation, such as Ericsson, Nokia, or Ionos, the stack layer accordingly indicates Mobile network vendor or Cloud service provider. As this perspective looks at the stack from the MNO's view, the models do not include the nuance where the MNO, the mobile network vendor and/or middleware vendor make use of any third-party vendors to supply parts to them to build up their services, e.g. buying servers and other hardware from companies like DELL, HP, Lenovo, etc.

During the interviews it became clear that mobile operators often use models in parallel, depending on the combination of CNFs they are using, so one model for CNF-x while using another model for CNF-y. In this approach, the CNFs interact with each other on a horizontal level, typically while hosted in the same mobile operator data centre.

3.2.1.1. Model 1

In the first Model, the MNO has its own data centre, at its own physical location. This data centre then becomes the basis for the rest of the cloud stack to be hosted on it. It is seen quite often (in 5 of the 7 Models) that the MNO owns its data centres. In Model 1, the rest of the stack is then provided by the mobile network vendor, including the physical infrastructure (e.g. servers, storage, networking) up till the containers (Kubernetes) and the CNFs. Since the cloud network has been hosted on the operator's own data centre, this deployment model can be categorized as a private cloud deployment which has been hosted on premise.

In such a model, the system integrator is typically the mobile network vendor. However, it may also be a third-party system integrator like Accenture or Capgemini.

3.2.1.2. Model 2

The second Model is similar to the first one. The difference is that, in addition to the data centre, the MNO also provides the physical infrastructure (e.g. servers, storage, networking), on which the rest of the stack will be hosted. The mobile network vendor then provides the software up till the containers and the CNFs. In this model, the deployment model can be also categorised as a private cloud deployment, which is hosted on premise.

3.2.1.3. Model 3

With the third Model, the role of the MNO remains the same as with the second model, however, there is an additional party involved: a middleware vendor. With this model the MNO selects a middleware vendor like RedHat, VMware by Broadcom, Wind River, on which they want their CNFs of one or more mobile network vendors of their mobile core to be hosted. In this Model as well, the deployment model can be categorized as a private cloud deployment, which is hosted on premise.

In such a model, the system integrator is typically the mobile network vendor. However, it may also be a third-party system integrator like Accenture or Capgemini.

3.2.1.4. Model 4

The fourth Model is different from the first three in that it includes a cloud service provider. The role of the MNO is the same as with the first model: it hosts the stack in its own data centre. But instead of the rest of the stack being provided by the mobile network vendor, the mobile network vendor only provides the CNFs. The physical infrastructure up till the container platforms is provided by a cloud service provider, such as Amazon or OVHcloud. In this Model as well, the deployment model can be categorized as a private cloud deployment, which is hosted on premise.

In such a model, the system integrator is typically the mobile network vendor or the cloud service provider.

3.2.1.5. Model 5

In the fifth Model, the role of the MNO changes as it does not provide any part of the stack. The first two layers of the stack, i.e. the housing and the physical infrastructure, are provided by a cloud service provider. On top of these two layers is a middleware vendor that provides a containerized platform on which the CNFs from a mobile network vendor are running. This deployment can be categorized as either a public cloud or a private cloud deployment depending on the service purchased from the cloud service provider (as defined in Section 3.1), and is hosted off premise.

In such a model, the system integrator is typically the mobile network vendor or the cloud service provider.

3.2.1.6. Model 6

Within the sixth Model, the MNO also does not provide any part of the stack. Compared to model five, there is no middleware vendor involved, and the cloud service provider provides a bigger part of the stack, namely from the housing up till the containerized platforms. The CNFs of the mobile network vendor are running on top of the platform provided by the cloud service provider. This deployment can be categorized either as a public cloud or private cloud deployment depending on the service purchased from the cloud service provider and is hosted off premise. In the interviews, this model and Model 4 have been mentioned in the context of a recent practical implementation [14], where they are used in parallel to a Model 1 implementation. Depending on the location of the network functions (in particular the UPF), this fits Model 4 or 6.

In such a model, the system integrator is typically the mobile network vendor or the cloud service provider.

3.2.1.7. Model 7

Within the seventh and last Model, the MNO provides most part of the stack itself, from housing all up to the containerized platform like Kubernetes. The CNFs of the mobile network vendor then need to be integrated into the container platform of the mobile network operator. This deployment model can be categorized as a private cloud deployment which is hosted on-premises.

In such a model, the system integrator is typically the mobile network vendor or the MNO. However, it may also be a third-party system integrator like Accenture or Capgemini.

3.2.1.8. Analysis

A key observation from the interviews is that there is a range of models that operators use, described in the previous sections. Mobile operators also can completely change from one model to another at a considerable effort and cost, as is the case in any migration between vendors and providers.

While the models in the sections above are described individually, in practice the MNO often uses different models in parallel. In almost all cases, this means that they use one cloud stack for one set of CNFs (say, the UPF, AMF and SMF, and use another cloud stack for other CNFs (including, say, the Unified Data Management (UDM)). This is shown in the left-hand stack in Figure 5. Typically, both cloud stacks are hosted in the same data centre and the communications between the CNFs that are required to make the 5G network function are made within in the data centre. In this approach, each CNF needs to be integrated with one cloud container platform.

The right-hand side of the figure shows another approach that, according to our interviews, is much less common. Here, individual CNFs are hosted on both cloud stacks in parallel, requiring them to be integrated with two cloud stacks. This integration is more complex as it needs to absorb the versions of Kubernetes and potential additional plug-ins that the CNFs depend on. In yet another approach, not shown here, CNFs from two (or more) different vendors are hosted on the same cloud stack. This also involves handling of different requirements for Kubernetes versions and plug-ins, but now from the CNF perspective.

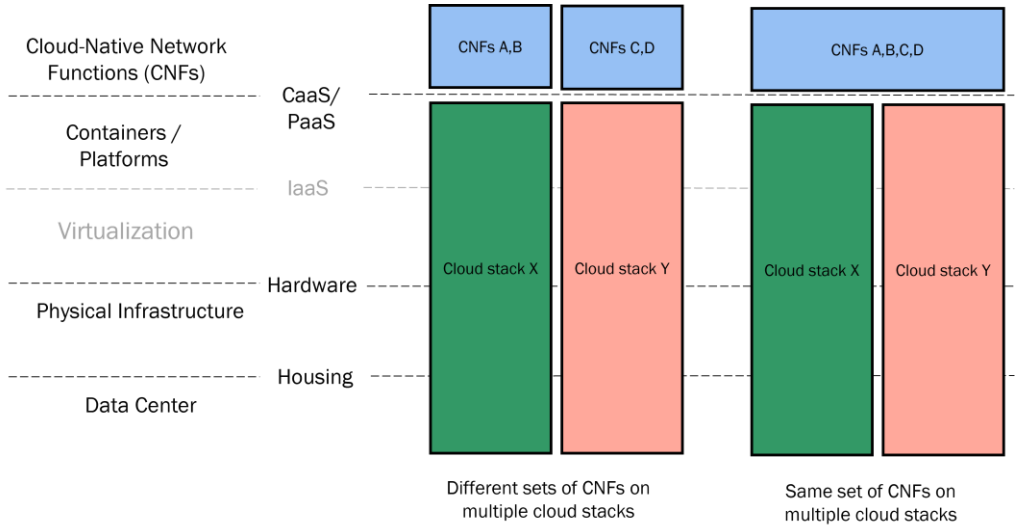

Figure 5. Parallel use of multiple clouds for CNFs.

Our interviews show that mobile network operator often use Models 1 and 2 as a basis and combine them with other models. This shows that the traditional model where the mobile network operator has a mobile

network vendor, the supplier of an integrated solution has also found its way into the new cloud-based technology generation. The models with a role for public cloud service providers (4, 5 and 6) are recognised in the interviews but are at the moment not used in the Netherlands. This is also true for Model 7 which is only used by (very) large operators: the considerable integration effort and investment make this model less attractive for many smaller and mid-size operators.

With the supply chain view, it is important to remember that the models present who is "supplying" the service, and not who is the OEM for the service. For example, in Model 3, if the mobile network vendor integrates the software modules of the middleware vendor in its own product, then we fall back to Model 2. This approach can be recognised in the collaboration between Nokia and Red Hat [15]. As another example, if the operator itself integrates the middleware modules in his own stack, then we are in Model 7.

The interviews show that the companies that provide the container layer also take care of the virtualisation layer below that. Thus, there is no inter-company interface between these two layers. The IaaS interface has therefore been greyed out in the figure.

Another upcoming architecture recognised during our interview is to skip the virtualisation layer and run the containers with the CNFs directly on the hardware layer to improve performance. Skipping the VM hypervisor layer results in less overhead caused by the virtual machine (VM) hypervisor layer and more resources available for the CNF layer, improving performance. Setup, configuration and scaling however, are more complex compared to a setup on top of the VM hypervisor layer, as that layer takes care of that. So, this setup is suitable for high-performance CNFs, for example a UPF or O-RAN.

As a final point, the interviews have not shown the use of the SaaS models within MNOs for CNFs. In that model, one company would offer the whole stack from hosting up to and including the CNFs to the mobile network operator as a service. In other sectors, for example office productivity tools like SharePoint, this is an established model. This is of course not to say that the SaaS model for CNFs cannot be introduced in the future for mobile operator networks. It has been tried with limited success in private networks and has also been seen as a model in use within some MVNOs. [16].

3.2.2. Operational perspective

Section 3.2.1 above described the models from the supply chain point of view. It is equally important to look at the operational or management view. This view focuses on who manages and operates the stack once it has been deployed. It is important to note that in the end the MNO is responsible for managing the stack as it is responsible for providing 5G/6G services to its customer. Thus, the final responsibility always rests with the MNO. However, the responsibility to operate certain layers of the stack may be delegated by the MNO to different service providers in different models.

To describe this operational view, we divide the management and support of the stack into the three well-known categories of First Line, Second Line and Third Line Support. First Line Support monitors the health of the infrastructure and handles basic issues, mostly done by a Network Operations Centre (NOC). Second Line Support addresses more complex technical problems (like network connectivity issues or complex software malfunctions) requiring advanced expertise, often from the vendor or software supplier. Third Line Support involves specialized engineers who resolve the most critical system failures, infrastructure issues, and complex technical challenges with in-depth knowledge of the telco cloud platform requiring for example deep code-level knowledge. In fields where security is a big concern, like in defence and military, it is seen that the cloud services from the cloud service providers may be air-gapped. However, this is not common practice in the telco sector.

3.2.2.1. Operational view variants for Model 1

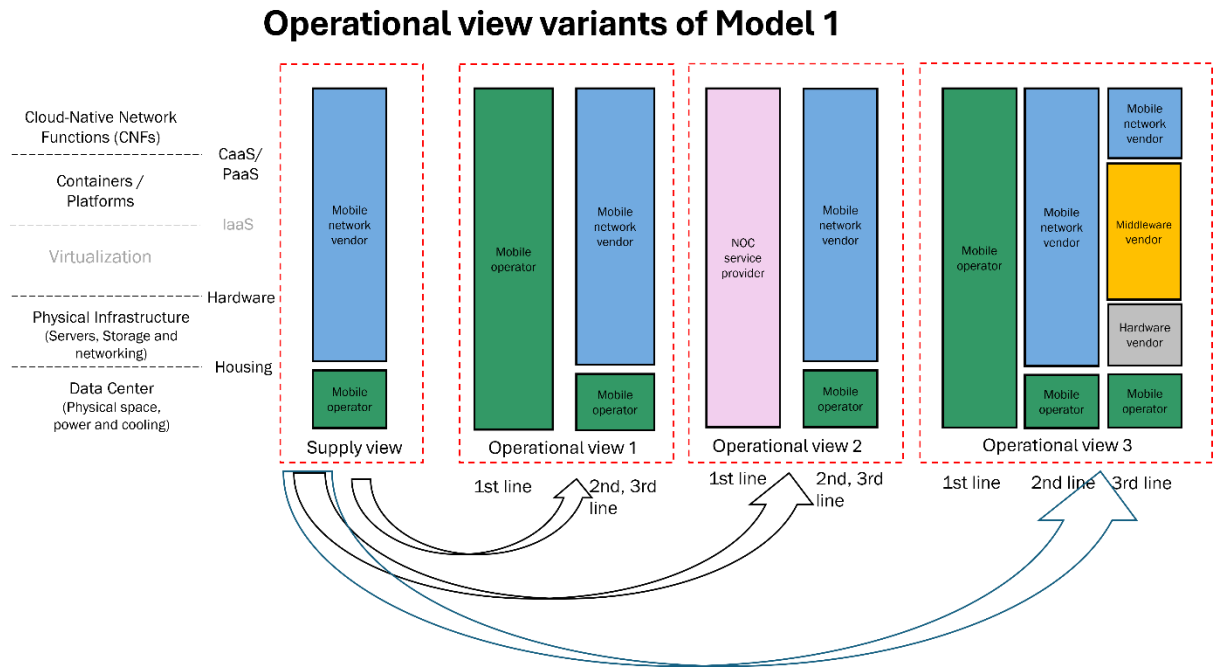

Figure 6: Operational view variants corresponding to Model 1

Model 1 of the supply chain view discussed in Section 3.2.1.1 shows that the data centre and housing are provided by the MNO while all other stack layers are provided by the mobile network vendor. For the operational control of the stack, the interviews and desk research point to three possible models (Figure 6). In the first operational view variant, the MNO is responsible for the First Line Support. This means that maintaining the health of the network and handling basic issues are done internally by the MNO. When those issues are not resolved in-house, the Second and Third Lines Support stacks fall back to the same view as the supply view, i.e., the supplier of that particular layer of the stack is also the operational support provider in this case.

In the second operational view variant, we see that the First Line Support is taken up by a separate NOC service provider. This could be companies like ServiceNow, INOC, or Google, Ericsson, or Microsoft. The Second and Third Lines Support fall back to the same stack view as in case of the supply chain model, similar to operational view variant 1. However, it is possible to split the Second and Third Lines Support, which is what we see in variant 3. Here the Third Line Support involves the suppliers that the mobile network vendor used to provide its services: a middleware vendor and a hardware vendor. When the issues can no longer be resolved by the mobile network vendor, it must go back to those vendors that it used to build up its services. When issues run deep, the responsibilities fall back to original provider of the services of the hardware parts involved. Thus, it is always possible to further detail out these models depending on the depth of the issues and the number of vendors involved within the provided service. Note that in operational variant 3 the First Line Support shows the MNO; however, there is also a variant 4 (not shown) where a NOC service provider does the First Line Support.

3.2.2.2. Operational view variants for Model 2

Similar to Model 1, the Model 2 has three possible operational view variants (Figure 7 above). The first two options again combine the Second and Third Line Support, with the difference that the First Line Support could be provided either by the MNO itself or by a NOC service provider. In the third variant, the Second and Third Lines Support have been split up in the same way as for model 1 in the previous section. This split now incorporates the middleware vendor and a hardware vendor that were used by the mobile network vendor and MNO, respectively, to assemble that layer in the stack. The third variant shows the First Line Support as the NOC service provider, but again this could also be the MNO.

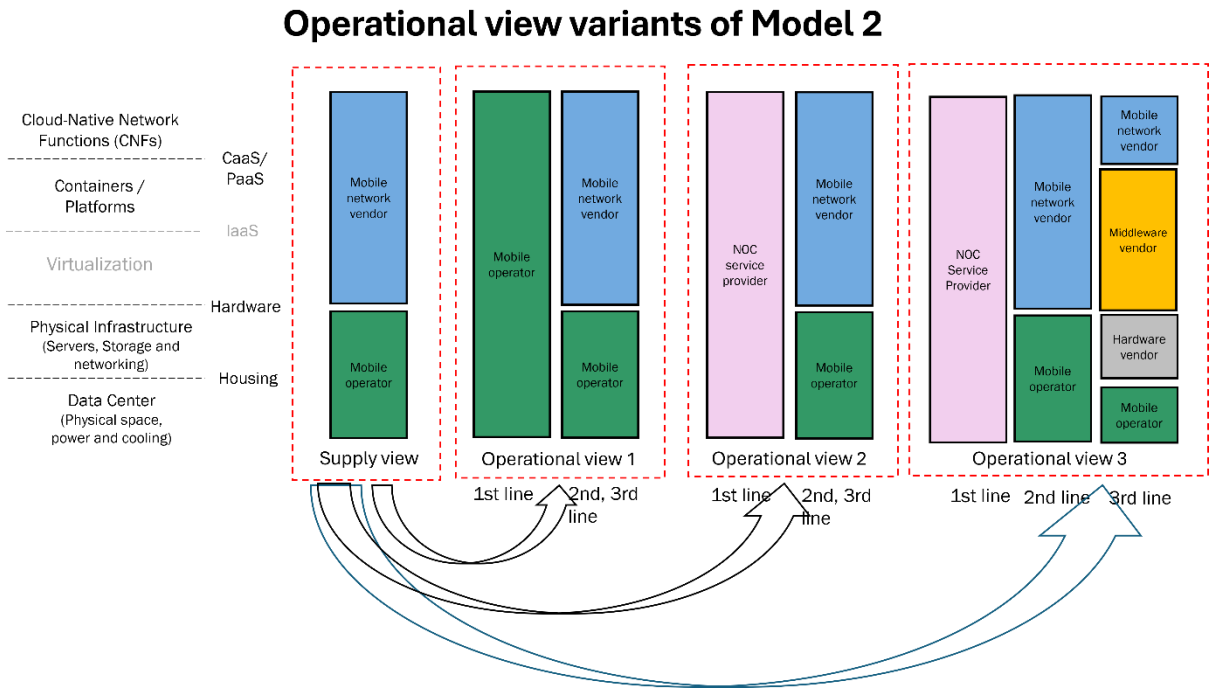

Figure 7: Operational view variants corresponding to Model 2

3.2.2.3. Operational view variants for Model 3

The operational view variants for Model 3 are similar to the ones for Model 2 (Figure 8 below). The first two variants show that the First Line Support could be provided either by the MNO or the NOC service provider. For the Second Line Support, the stack falls back to the supply model, i.e., the supplier of the different layers is also providing the Second Line Support. In the third variant, the First and Second Lines Support stays the same but the Third Line Support includes the hardware vendor, who will diagnose and resolve the problems when the MNO is not able to.

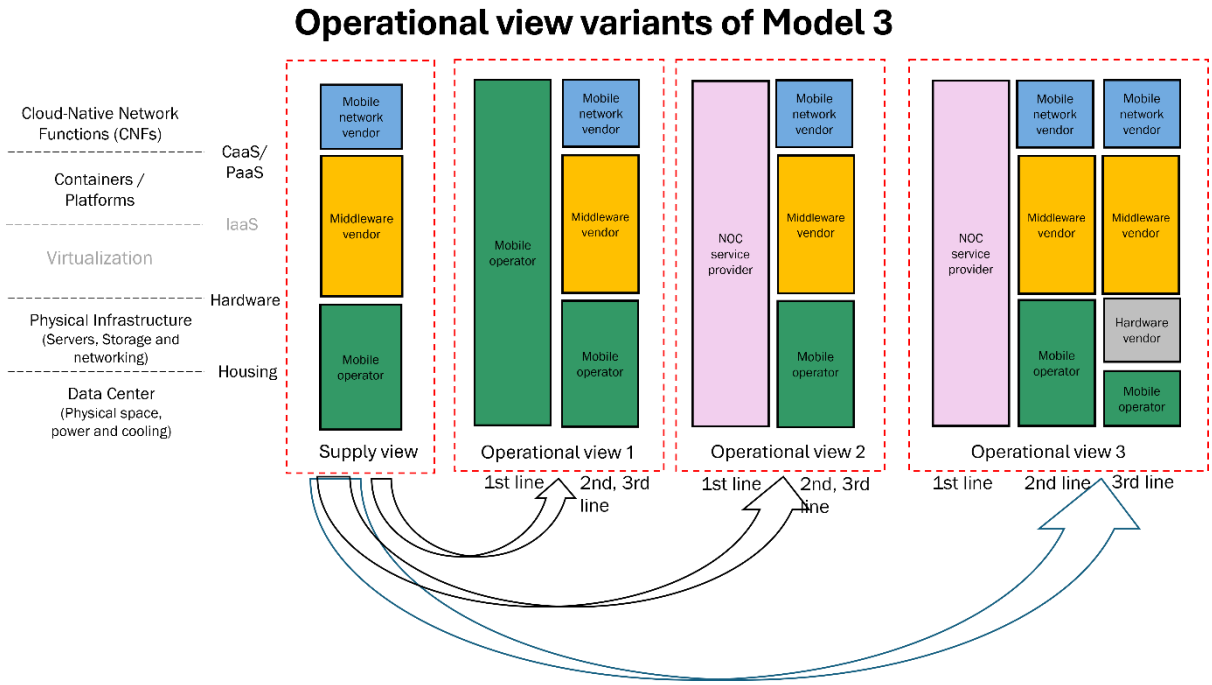

Figure 8: Operational view variants corresponding to Model 3

3.2.2.4. Operational view variants for Model 4

Within Model 4, we see that only two operational variants have been presented (see Figure 9 below) – one where the First Line Support is provided by the MNO and the other where the First Line Support is provided by the NOC service provider. The Second Line Support in both variants follows the supply stack view. However, one might wonder why there is no third variant present here. This is because from the MNO's perspective, once the cloud service provider is involved in the problem resolution and is also the supplier of the layers, the MNO has a limited view from that point on. If the problem cannot be solved by the cloud service provider internally, it would need to engage other parties to help with the resolution. However, while the final responsibility for the service lies with the MNO, as far as operational control is concerned here it still lies with the cloud service provider. This also highlights the dependencies that exist on the cloud service providers, as the operational control shifts further away from the MNO when problems are not solved within First Line Support.

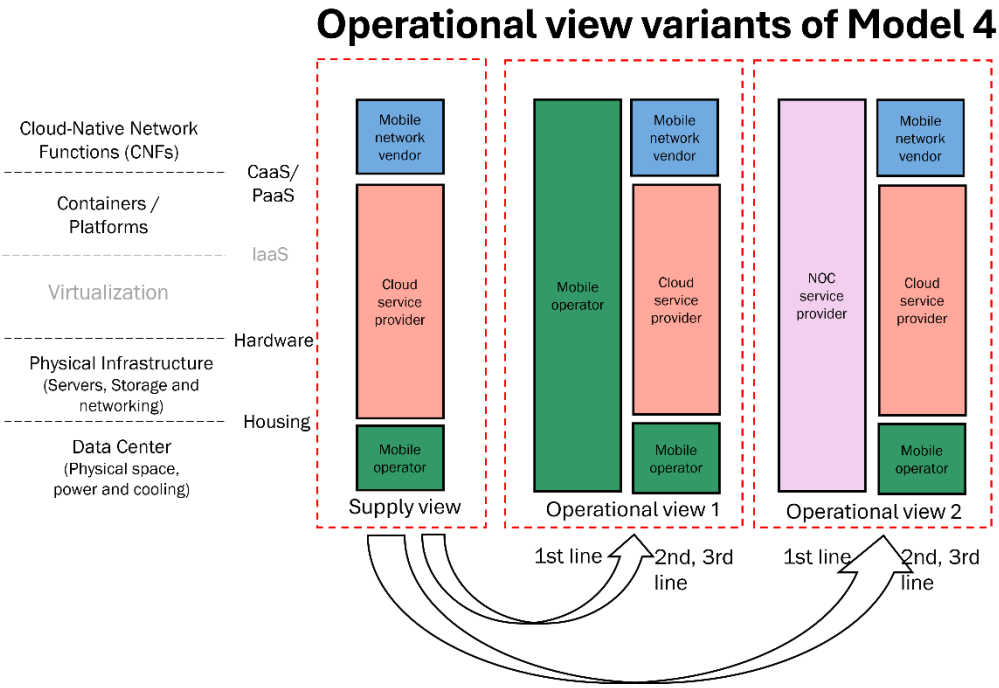

Figure 9: Operational view variants corresponding to Model 4

3.2.2.5. Operational view variants for Model 5

The operational view variants for Model 5 are similar to that of Model 4 (see Figure 10 below). Either the MNO or the NOC service provider could provide the First Line Support, and the Second Line Support mimics the supply stack. However, what is interesting in the operational variants of this model is that this is the first model where the First Line Support isn't entirely provided by the MNO or NOC service provider; it also includes the cloud service provider. This is because the cloud service provider is providing the two lowest layers of the stack, which are hardware layers. Since this stack is housed on the public cloud, or a private option but still not within the premises of the MNO, it would be difficult for the MNO or a third-party like the NOC service provider to diagnose and resolve any issues here. The physical hardware must be operated and maintained by the party that supplies it, and thus even the First Line Support for those layers must come from the cloud service provider.

It is not possible to break down the stacks further to create a third operational variant as once the problem has reached the cloud service provider or the middleware vendor, it becomes a black box for the MNO. They may engage other parties and vendors to resolve the problem, but the operational control still lies with them.

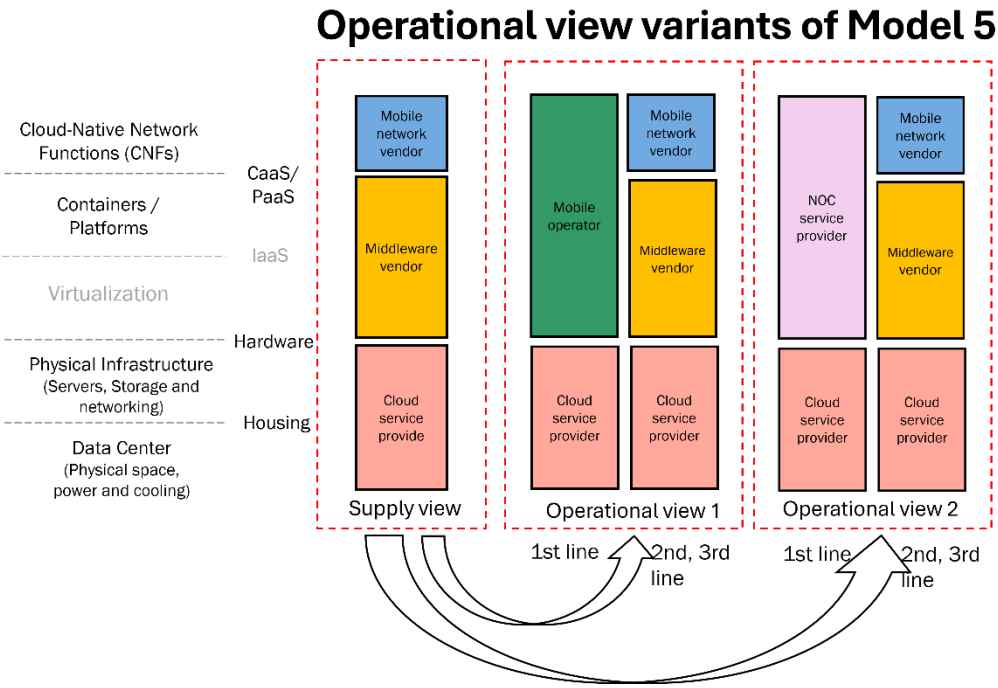

Figure 10: Operational view variants corresponding to Model 5

3.2.2.6. Operational view variants for Model 6

Model 6 is very similar in its operational view variants to Model 5 (see Figure 11 below). The two lowest layers of the stack, i.e. the hardware layers, must receive the First Line Support from the supplier, which in this case is the cloud service provider. The other layers of the stack for the First Line Support could then be with the MNO or the NOC service provider. The Second Line Support for both variants falls back to the supply model and the cloud provider taken on a greater share of operational responsibility.

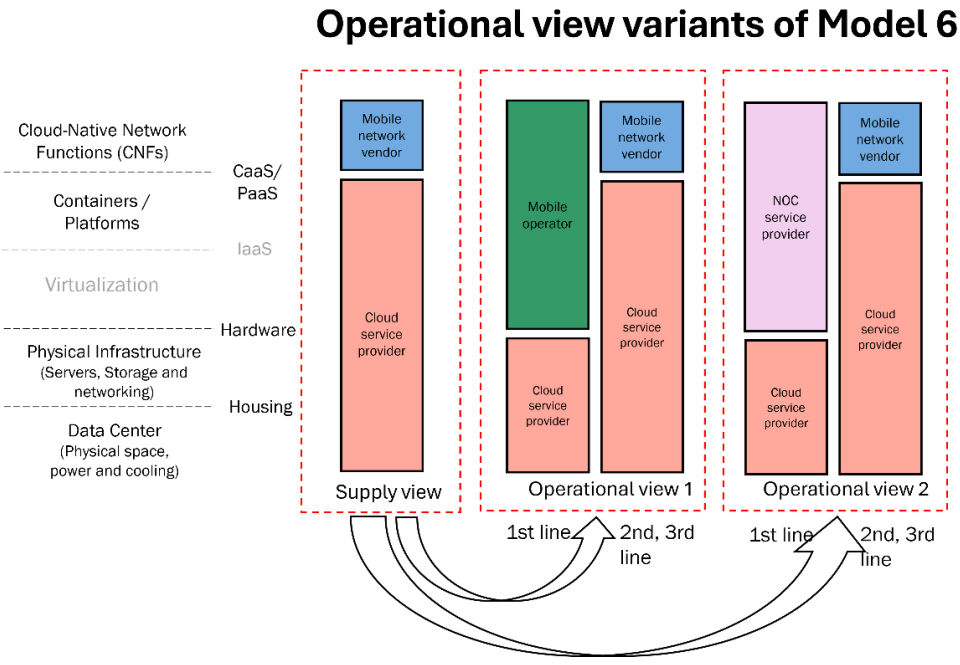

Figure 11: Operational view variants corresponding to Model 6

3.2.2.7. Operational view variants for Model 7

In Model 7, a large part of the stack lies with the MNO. Hence the operational view includes the First Line Support being provided entirely either by the MNO itself or by a NOC service provider. The Second Line Support in the first two operational variants falls back to the supply view, as seen in all other models as well. In the third variant, we break down the MNO's part of the stack to include the middleware vendor and hardware vendor. This is because if the problem cannot be resolved at the operator's side, it must then lean on the vendors that helped to build up the stack (see Figure 12 below).

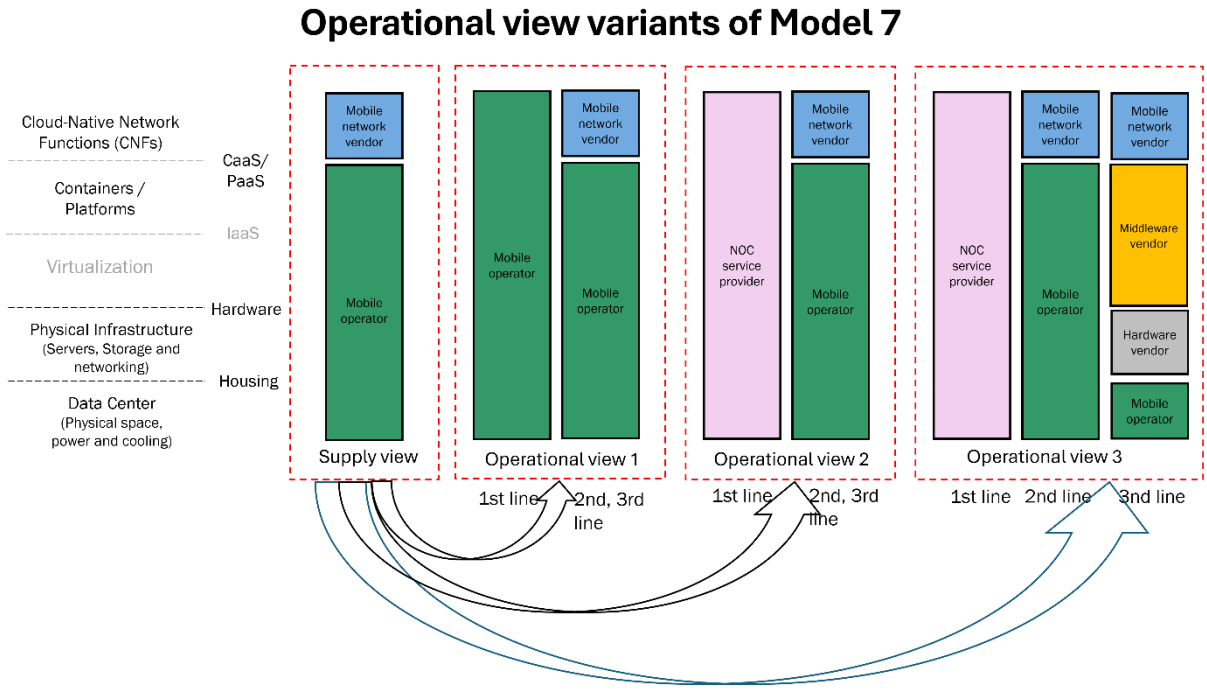

Figure 12: Operational view variants corresponding to Model 7

3.2.2.8. Analysis

The operational variants presented in the section above show that for every supply model there can be several operational view variants. In our analysis, in most cases First Line Support is provided either by the MNO itself or by a NOC service provider engaged by the MNO. This is where the MNO retains the operational control for problem resolution. As we go further into the support lines, we notice that the supplier for the specific hardware becomes involved. One could go into further level of detail, as a middleware vendor, for example, can again be dependent on the availability of updates in open source modules. Dependencies on open source modules can go several levels deep and, therefore, are difficult to trace, while they are still important for the operational control. Another layer of complexity is added when intermediaries/resellers provide certain layers of the stack. For example, F2 purchases services from AWS, adds services on top of it and then sells it on to an operator/vendor.

The operational variants also demonstrate that no MNO is able to control the complete supply chain in any of the supply models. In terms of operational control, MNOs always experience dependencies on different supplies. The differences between the models are in the extent to which an MNO is dependent on suppliers and in the profile of those suppliers. Open source does not resolve the problem either: as mentioned above, dependencies reach deep in the stack and are even difficult to trace for an MNO.

3.3. Definition and standardisation of interfaces

The previous section shows multiple different cloud service and deployment models which, depending on the type and requirements of the CNF, are often combined in order to provide a full 5G core network. Combining these CNFs as well as the different service and deployment models requires well defined and standardized interfaces.

For horizontal interoperability on the CNF layer, e.g. the 5G core CNFs, 3GPP is standardizing interoperability between different implementations. This is mainly done by standardizing the interfaces of the different 3GPP network functions and the information that is exchanged over these interfaces. The implementation of these functions is left to the (mobile) network vendors.

For vertical integration of CNFs with cloud infrastructure however, there is no standardization like done in 3GPP. Instead, this is driven by a community effort within the Linux Cloud Native Computing Foundation (CNCF) [17] to have interoperability by using the same implementation, e.g. Kubernetes. Hence, Kubernetes has become the de facto standard implementation to be used to host containerized applications/CNFs. This de facto standard helps MNOs as they can choose and also move between different cloud stacks. Moving to another cloud stack comes with significant cost, as is the case with any substantial network migration, but it is important to appreciate the degree of interoperability and standard software engineering practices that currently exists through Kubernetes. The introduction of technically more advanced multi-cloud models, such as hosting individual CNFs on two cloud stacks in parallel (right-hand side of Figure 5), would require interoperability at deeper levels to handle the versions of Kubernetes and potential additional plug-ins that the CNFs depend on.

Next to the Linux CNCF effort, there exist further initiatives to promote interoperability and reduce costs for the telecommunications industry, like:

- Project Sylva [18] which is an open-source initiative under Linux Foundation Europe aiming to create a standardized, production-grade cloud software framework for telecommunications (telco) and edge applications. One of their goals is to stimulate collaboration among European operators, vendors, and cloud providers. Building on existing open-source components to offer an interoperable, secure, and scalable cloud stack.
- Project Anuket [19] which is an open-source initiative under the Linux Foundation Networking merging the Cloud iNfrastructure Telco Taskforce (CNTT) and Open Platform for Network Function Virtualization (OPNFV) to standardize Telco Cloud platforms. Their goal is to accelerate the deployment of network services by providing reference cloud infrastructure models, architectures, conformance tests, and open-source tools.

3.4. Evolution to 6G with edge, Open RAN and AI RAN

Section 3.2 described the different models by which a core network (and its functions) can be provided in a cloud-based manner. In 6G mobile networks, cloud will be used wider than just in the core section of the network: it will extend to the edges of the network. This also means that the cloud stacks discussed earlier, and potentially new variants, will find their way to new locations in the network (Figure 13).

Our desk research and interviews show three technical drivers for deployment of cloud infrastructure:

- Open RAN, which aims to improve flexibility and interoperability of Radio Access Networks by splitting the RAN components and making their interfaces open. The O-RAN alliance [20] has developed an architecture for the RAN consisting of three main components: the Radio Unit (RU), connected to the antenna, the Distributed Unit (DU), linked to the RU via a so-called fronthaul interface and the

Centralised Unit (CU) that links to the mobile core network. For this paper, it is important to note that the DU and the CU are expected to be cloudified: their subfunctions would run on the cloud stack similar to the CNFs discussed earlier. Also, the introduction of AI to the RAN to improve efficiency and capacity of the radio interface is expected to need a cloud stack to support AI compute.

- Edge processing for users' apps. On the same or on different locations as the cloud stacks for O-RAN, cloud infrastructure that provides compute for applications of end users can be placed. There can be different motivations for this. A classical argument is to reduce the latency for applications. Though our interviews did not render specific examples, common examples are vehicle safety, offloading compute to edge for online gaming and extended reality applications but also the introduction of AI and Generative AI. Other motivations can be to reduce the data traffic in higher segments of the network and to process data locally and prevent it from leaving a given geographic area (data sovereignty).
- AI-RAN, promoted by the AI-RAN alliance [21], which is an umbrella term for different uses of AI linked to the RAN. They would all include a cloud stack to support the AI compute. AI-for-RAN uses AI to improve the efficiency and capacity of the radio interface. AI-and-RAN aims at concurrent use of AI-RAN and of Generative AI workloads that mobile operators have on the same RAN infrastructure. AI-on-RAN takes this further to include Generative AI workloads from customers from (consumers, businesses and governments). Note that these AI functions can be hosted at locations also used for Open RAN and the edge processing for users' apps.

For this paper, the main observation is that role of cloud in and around 6G mobile networks will become larger and, therefore, also the weight of policy considerations on the topic.

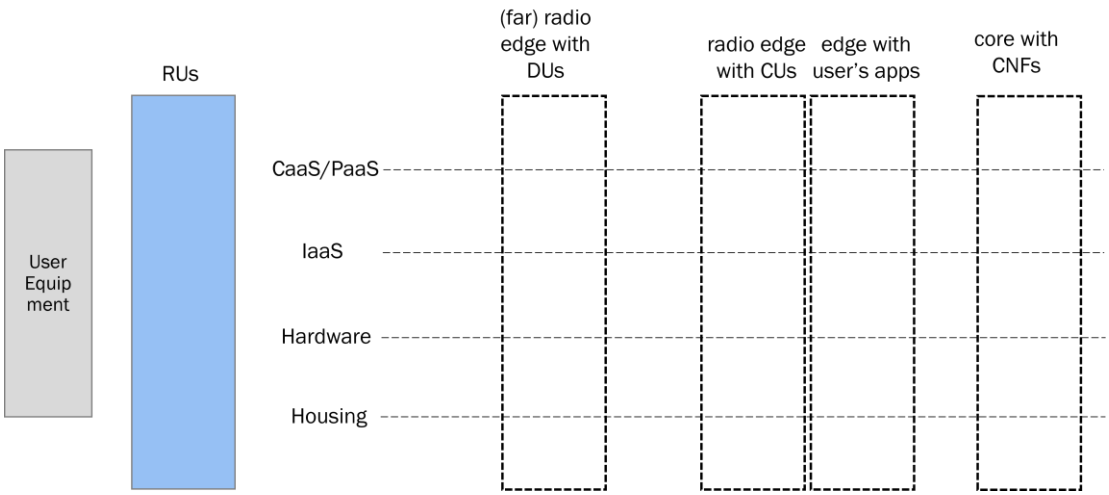

Figure 13. Cloud stacks in the edge-cloud continuum for 6G.

4. Mapping technology to policy

4.1. Policy learnings for telco cloud from 5G

Specific technical characteristics of 5G and its interplay with telco cloud, as described in Section 2, attracted the attention of policymakers and regulators that analysed what they meant for policy and regulation. An early and comprehensive analysis of the changes induced to the telecom ecosystem by the deployment and development of 5G was made by BEREC. In 2022, BEREC [22] observed that 5G network softwarisation, virtualisation and automation would require adaptation of the traditional telecom players to demands of the technology and new ways of working. In 2024, BEREC [23] found that cloud technology changes how telecom services and networks under 5G are developed and delivered to customers and plays an increasingly important role for mobile. BEREC points out that, at the moment, "the extent to which hyperscalers will penetrate further in the value chain is still unclear" [23] because they are far from achieving the capillarity of the telecom network and are not interested in competing on the traditional telecom market. On the other hand, hyperscalers can provide verticals with value-added services independently from telcos, which means that they can compete in some segments. Based on these and other observations, BEREC concludes that regulators must remain vigilant to potential competition issues both due to partnerships between telcos and cloud providers and due to the presence of hyperscalers across the complete 5G ecosystem (e.g. risk of leveraging market power to adjacent markets, lock-ins) [23]. For the development of 6G and related cloud, BEREC points out the importance of continuing to address bottlenecks and steer the market towards more openness and interoperability [23]. Portability, switching and multi-cloud are important attention points, already somewhat covered by legislation. However, BEREC expects hyperscalers to remain central players in the cloud ecosystem – and by extension in the cloud-native 6G. The prevalence of third-country operators among hyperscalers may also cause security and digital autonomy concerns as pointed out by the Draghi and Eurostack reports.

The 2024 Draghi report [5] pointed out that, with softwarisation and virtualisation of telecommunications, the reliance on third-country companies grows, and the EU may become more vulnerable regarding its digital autonomy cyber-resilience, security of strategic infrastructures and protection of data of citizens and businesses. While the Draghi report did not specifically focus on telco cloud, it analysed the cloud market in general pointing out the dominance of US hyperscalers and the trailing position of European companies. The Eurostack [24] report calls for learning lessons from the 5G security challenges by ensuring that 6G architecture can isolate security of certain elements (e.g. core-of-government information/ communications), embedding this approach in business models and regulation. The scalable, interoperable and unified cloud infrastructure must be fully under the EU jurisdiction, strongly aligning with the EU's green transition goals and providing resilient and robust performance under high demand.

4.2. Relevant legislative framework

While limitations to portability and switching, lock-ins and other issues mentioned in Section 4.1 remain potential risks for telco cloud, they have not yet materialised in practice. As demonstrated in Section 3.2, there are several supply models of telco cloud and operational variants within them used by MNOs. Our interviews confirmed that all of the models are used, frequently they are used in parallel for different CNFs. MNOs can switch between models, subject to usual costs and constraints related to changing technology providers. We did not conduct a proper market analysis in the sense of competition law, as this is beyond the scope of the FNS work. However, none of the conducted interviews or desk research identified bottlenecks or questionable practices in telco cloud at this point in time.

Yet, market, business and deployment models can evolve. In particular, the trend to using more SaaS could introduce bottlenecks in the future. This is why an analysis of legislative instruments targeting economic concerns identified by various policy reports in relation to cloud services is warranted. As analysed in Section 2.4, these concerns include interoperability, competitiveness and digital autonomy. Interoperability and competitiveness are in the focus of the Digital Markets Act (DMA) and Data Act (DA), while the NIS-2 Directive and EU 5G Toolbox touch upon (cyber)security from the perspective of supply chain.

Many other EU legislations regulate other aspects of cloud computing services. For example, the Digital Services Act regulates the obligations of hosting providers with regard to content. However, we do not consider such other aspects relevant for our research question and, therefore, do not cover these legislations here. While recognising the relevance of various industrial policy measures (e.g. IPCEI Next Generation Cloud Infrastructure and Services (IPCEI CIS) [25] and the future EU Cloud and AI Development Act [26]) to increase European competitiveness and digital autonomy, we do not analyse them because these measures are still to bear fruit. Lastly, we also did not analyse the relevant Dutch national legislation (e.g. Regulation on the security and integrity of telecommunications - Regeling veiligheid en integriteit telecommunicatie) as it has been analysed in other projects.

The sections below present a short version of the analysis of the legislation. A longer version of the analysis is contained in the Annex to this report.

4.2.1. Digital Markets Act likely of little relevance for telco cloud

The DMA [27] is a competition law instrument primarily concerned with preventing dominant providers of core platform services from abusing their market power. A company must be first designated as a gatekeeper in order to be subjected to the DMA obligations. Until today, no provider of cloud computing services has been designated as a gatekeeper.[2] The DMA targets services that intermediate between business users and end users, but cloud computing in general lacks multi-sidedness (i.e. does not act as an "important gateway for business users to reach end users") [28]. Moreover, a telco cloud solely hosts the core network or the radio network of a mobile network (as explained in Section 1.1). It in no way intermediates between business users and end users, but provides tools and functions for the MNO to efficiently manage its network.

The Commission is empowered to adjust the methodology for the designation of gatekeepers, which may lead to designation of a cloud provider or even a telco cloud provider. If this happens, only the DMA obligations related to business users will be applicable to a telco cloud (i.e. because there are no end users). These obligations are the prohibition for a gatekeeper to bundle cloud computing with other core platform services, the prohibition to use business data of a gatekeeper's business user to compete against this business user and the obligation of provision of real-time access to data for business users.

While these gatekeeper obligations aim to increase competition and contestability of the market, none of them is relevant in the context of the telco cloud as can be seen from the deployment models and operational variants described in Section 3.2.

4.2.2. Data Act focusing less on functions relevant for telco cloud

By contrast to the DMA, the DA [29] applies to all cloud computing providers and aims to facilitate effective switching between providers and interoperability of cloud computing services, including when using several

[2] The criteria for the designation are contained in Art. 3(2) DMA. For the updated list of designated gatekeepers, please see: https://digital-markets-act.ec.europa.eu/gatekeepers_en.

such services in parallel (i.e. multi-cloud). However, the DA provisions on interoperability are limited and do not seem to be conceptualised for a telco cloud. The definitions of interoperability and switching are rather focused on the use of data and do not account for technical and functional interoperability. The DA also misses the nuanced approach to interoperability for different cloud service models [30].

The DA provisions on interoperability in multi-cloud are the same as the DA provisions on switching, and the switching provisions shall apply to interoperability *mutatis mutandis*, although it is not always clear how this is possible.

Cloud providers must refrain from inhibiting porting of customer's exportable data and digital assets. Porting is not defined by the DA, but, based on the context, it foresees the possibility for the cloud customer to freely move its data and digital assets between different clouds. For telcos using several clouds in parallel, the possibility to port data between different telco clouds is irrelevant as the actual data will be processed at a much higher layer, to which telco companies are unlikely to have access. However, porting of digital assets – which seem to mean also containers or CNFs – in the sense of running the same CNFs on two or more clouds may be a possible scenario, although we have not encountered it in practice during our research. Currently, MNOs run different CNFs on different clouds for the same network, however, in the future there may be a hypothetical scenario of running the same CNFs on different clouds in parallel.

The source cloud provider shall not inhibit its customers from achieving functional equivalence in the use of the new cloud service of the same service type. Functional equivalence means re-establishing, on the basis of the customer's exportable data and digital assets, a minimum level of functionality in the environment of a new cloud service of the same service type after switching. The destination cloud service then delivers a materially comparable outcome in response to the same input for shared features supplied to the customer. Under the DA, cloud providers can only be expected to facilitate functional equivalence for the features that both the source and destination data processing services offer independently.

In the multi-cloud use, it is questionable to what degree the cloud services are of the same service type. Due to the lack of clear definitions of the key elements of what constitutes "same service type", whether two or more cloud services are same service types has to be determined on a case-by-case basis depending on main functionalities and primary objectives of these services. Under the DA, only IaaS providers have an obligation to facilitate functional equivalence. However, this is meaningless in the context of the telco cloud because, as shown in Section 3.2, the IaaS interface is not used in practice. The IaaS seems to lose significance in the sector as the trend goes to using containers without virtual machines on bare metal.

Lastly, the cloud provider should not inhibit the customer from unbundling IaaS from other cloud services, which may be necessary for the customer to achieve functional equivalence in IaaS. However, according to our research, the IaaS interface is not used in the telco cloud and not relevant in the environment with containers or Kubernetes on bare metal. Therefore, also this obligation is not relevant for the telco cloud in the multi-cloud use scenario.

4.2.3. Potential to increase digital autonomy in telco cloud via cybersecurity measures

As a part of digital infrastructure and a sector of high criticality, cloud computing is subject to the cybersecurity requirements under the **NIS-2 Directive** [31]. Providers of cloud computing must comply with enhanced risk management measures, perform security tests and report significant cybersecurity incidents. The NIS-2 Directive does not restrict the choice of suppliers or service providers for sectors of high criticality a priori. However, companies in such sectors must take appropriate technical, operational and organisational measures to manage risks to the security of network and information systems that they

use for their operations or for the provision of their services. Such measures must ensure a level of security of network and information systems appropriate to the risks posed, taking into account – among other things – the degree of the entity's exposure to risks and likelihood and severity of incidents. Such measures aim to protect network and information systems and their physical environment from incidents and include supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.

Although the NIS-2 Directive focuses on cybersecurity, it can have an indirect effect of improving digital autonomy in telco cloud due to the requirement of assessing and mitigating risks within the supply chain of telco operators. Depending on the national transposition, this requirement may lead to diversification of the supply chain and/or rejection of certain suppliers.

The NIS-2 Directive may have an even stronger impact on digital sovereignty when it is eventually combined with an active cybersecurity certification for cloud services. Under the NIS-2 Directive, Member States have the option to oblige telcos to use only cloud service providers that are certified under an EU cybersecurity certification scheme. The relevant certification scheme – **European Cybersecurity Certification Scheme for Cloud Services (EUCS)** – is in preparation by ENISA since 2019 [32]. The draft EUCS has been revised several times and is still far from formal adoption due to a long-standing discussion on the potential inclusion of sovereignty requirements in the EUCS.

The first EUCS draft of December 2020 [33] required cloud service providers to be transparent about the geographical location(s) of all system components, on which their customers' data is stored and processed, and the laws applicable to it. The revised 2023 draft EUCS[3] proposed an additional high+ assurance level, which is possible only for providers with the registered head office and the global headquarters in the EU and without direct or indirect control by third-country companies. Another requirement for the high+ assurance level was that all system components, on which the cloud service provider or its sub-service providers stored and processed data, had to be in the EU; and the management, monitoring and support had to be provided only from EU locations. Individual, precisely specified support activities were allowed from third countries only under exceptional circumstances. The 2023 draft EUCS proposed novel requirements going beyond traditional security controls. This version would have significantly limited the choice of suppliers for a telco cloud, possibly forcing companies to rethink their cloud deployment models and operational variants. The high+ assurance level was removed from the third draft EUCS of 2024[4], and the sovereignty requirements were limited to the obligation of transparency regarding the location of where customer data is stored and processed and to the obligation that cloud service providers must "operate primarily" within EU law and law of EU Member States [34].

In the specific context of 5G/6G and cloud, the **EU Toolbox for 5G Security** [35] is relevant as it links economic/ market developments to cybersecurity. The EU 5G Toolbox identified the risk of dependency on any single supplier within individual networks or lack of diversity on nation-wide basis and the risk of state interference through 5G supply chain. In connection with these risks, it foresees a pack of mitigating measures focusing on the ecosystem level and on the diversity of suppliers, but not specifically addressing (operational) control of the cloud stack as reflected in the models in Section 3.2 (i.e. operational variants of models). Also, cloud computing is explicitly mentioned only in the context of one technical measure, namely the requirement to use cybersecurity certification for non-5G-specific ICT products and services,

[3] The 2023 EUCS was leaked to news portal Politico. The text is not directly available anymore, but was widely discussed in various publications. The text is based on the reports of the time.

[4] The 2024 draft EUCS was also leaked. No final text of the EUCS has been published officially since the original first draft in 2020. For the analysis of the debates on the draft EUCS and positions of Member States, see [41].

thus linking it back to the future EUCS. Lastly, the implementation of the 5G Toolbox differs per Member State. National measures may in practice (indirectly) restrict the use of public cloud in telecommunication networks, especially for critical network elements, for instance, by setting technical requirements applicable only to telco networks.

5. Conclusions

5.1. Deployment models

The main motivation of this paper was to research the cloud stack deployment models used by MNOs and identify different types and roles of suppliers involved in the deployment. Our interviews and desk research show that Dutch mobile operators combine their CNFs, provided by mobile network vendors like Ericsson and Nokia, with several cloud stack models. They can choose and also move between different cloud stacks because of the well-established Kubernetes Container-as-a-Service layer between the CNFs and the supporting cloud stack. Moving to another cloud stack comes with significant cost, as is the case with any substantial network migration, but it is important to appreciate the degree of interoperability and standard software engineering practices that currently exists through Kubernetes. Also in the situation that the CNFs and the cloud stack are provided by the mobile vendor in a combined offering, the Kubernetes interface is used internally. This important role for Kubernetes is also reflected in the Sylva work on further streamlining Kubernetes for telco cloud.

At this moment, there is no SaaS offering to MNOs for CNFs in use, where the CNFs (and underlying cloud stack) are offered as a service to the mobile operator. This makes the situation for CNFs and telco cloud different from the situation in other sectors and application areas, like office productivity software, where the SaaS offering lead to concerns about lack of interoperability and potential for lock-in. In a scenario where SaaS offerings become dominant for CNFs, these concerns may also become relevant for telco cloud. This is the motivation to look at the existing and new policies in digital markets (see Section 5.2).

The mobile operators use different cloud stacks in parallel, where they run one set of CNFs on one cloud stack and another set of CNFs on another type of cloud stack. The cloud stacks are then typically connected in the mobile operator's data centre so that the CNFs can interact to perform their functions in the 5G core. The operators do not run one and the same CNF on different clouds. This would (at least in theory) improve their flexibility and reduce their operational dependence on the individual cloud stacks, but at the cost of substantially more operational complexity.

For the operational control of cloud stacks, there are many options for distributing the responsibilities for First, Second and Third Lines Support.

So far, there is no use of public cloud services for the CNFs in the Dutch mobile operator core networks. The examples from the US and from Germany are well-known and followed with interest. Our desk research and interviews point at performance and managing of subscriber data as factors that become more difficult to handle and control in public cloud services for CNFs. Note that for IT cloud, many mobile operators do make use of public cloud providers.

In the further evolution of 5G networks and in 6G mobile networks, cloud will be used wider than just in the core section of the network: it will extend to the edges of the network. This also means that the cloud stacks discussed in this white paper will find their way to new locations in the network and will be used for additional functions than the CNFs, such as those for the RAN and potentially for a range of other workloads from mobile operators and their customers. As a result, the importance of cloud stacks will grow further. This will be investigated further in another FNS deliverable following up on this white paper.

5.2. Policy instruments

Having understood the cloud stack deployment models currently used by MNOs, this white paper analysed how the relevant existing EU-level legislations can address the problems of dominance of big tech and digital autonomy – the main critical issues identified by leading policy reports for cloud.

The EU-level instruments aimed at market regulation and increasing competition are unlikely to make a difference for the telco cloud for two reasons. Firstly, a telco cloud provider is unlikely to be designated a gatekeeper under the current DMA definition.[5] Yet, even if this happens, the applicable obligations are irrelevant for the business model and operations in the context of a telco cloud as exemplified on the deployment models and operational variants. Secondly, the DA is more promising as it applies to any cloud provider. However, it rather focuses on interoperability of the data use and less on the interoperability of functions or technological interoperability, which are necessary in the parallel use scenario of a telco cloud. Only the obligations around porting of digital assets have a clear application to a telco cloud. Some of the DA provisions hinge on the distinction of three service models (IaaS, PaaS, SaaS) making it less flexible and future-proof in the face of technological development that combines and transcends such distinction. For example, some DA obligations apply only to IaaS providers, but as the deployment models show, IaaS does not play any role in the telco cloud due to the current trends towards using Kubernetes on bare metal.

With regard to digital autonomy, there are no dedicated legal instruments at the EU level. However, cybersecurity legislation recognises that (cyber)security risks may stem from deficiencies and dependencies of the supply chain of companies within sectors of high criticality. The NIS-2 Directive, therefore, requires risk assessment and mitigation measures that encompass the supply chain. The efficacy of the NIS-2 Directive in this regard could be strengthened once a cybersecurity certification scheme for cloud services is adopted and if such a scheme includes more specific "sovereignty requirements". Lastly, the EU Toolbox for 5G Security also addresses cybersecurity risks that may result from the supply chain and provides – mainly systemic and strategic – recommendations for their mitigation.

On a more general note, we observe that all analysed legal instruments look at cloud computing more generally and are not specific to the telco cloud, which has some special characteristics regarding its deployment and operation (as per Section 3.2).

Equally, almost all analysed instruments focus on the supply chain rather than operational control of cloud, whereas our research demonstrated that, in the telecom context, both are important and can result in competition or autonomy shortcomings. It also needs to be considered that, because a complete operational control is not possible for an MNO under either of the supply models, the risk-based approach to digital autonomy in telco cloud is likely to be more effective than the control-based approach. Risk identification, assessment and mitigation are key, while the understanding that residual risk may remain, even when relying on open source. In addition to such risks, MNOs need to think in terms of their liabilities and shape their supply contracting accordingly.

[5] We note that in November 2025, the European Commission launched market investigations related to potential designation of Amazon and Microsoft as gatekeepers for their general cloud computing services, despite not meeting the DMA gatekeeper threshold for size, user number and market position [48].

Annex

This annex contains a more detailed legal analysis of the relevant legislations and is, therefore, complementary to Chapter 4 of the paper.

Definitions of cloud computing under the DMA, DA and NIS-2 Directive

The definitions of cloud computing services under the three legislations discussed below differ (see Table below). Art. 2(13) DMA and Art. 6(30) NIS-2 contain the same definition, while the definition of cloud computing services under Art. 2(8) DA is considerably more precise and is closely aligned with the technical definition by the US National Institute of Standards and Technology (NIST) [36]. At the same time, the DA definition seems more pointed and limiting due to its greater level of detail. It is likely that the definition of the DMA and NIS-2 Directive can be interpreted broader and more services would fall under it. For instance, under models 1 and 2 there is no service offered to a customer, hence the Data Act does not apply.

Art. 2(13) DMA and Art. 6(30) NIS-2	**Art. 2(8) DA**
a digital service that enables on-demand *administration and broad remote* access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations	a digital service *that is provided to a customer and* that enables *ubiquitous and* on-demand *network* access to a shared pool of *configurable,* scalable and elastic computing resources of a centralised, distributed or highly distributed nature *that can be rapidly provisioned and released with minimal management effort or service provider interaction*

Cloud computing under the Digital Markets Act

The DMA is a competition law instrument and primarily concerned with the market power of big tech companies that provide core platform services – of which cloud computing service is one (Art. 2(2) (i) DMA) – in the EU. The DMA aims to pre-empt abuse of this market power and lower the risks of reduced contestability of certain markets, serious imbalances in bargaining power and unfair practices vis-à-vis users of core platform services.[6]

Hence, the DMA regulates the provision of cloud computing services only in certain circumstances, namely when they are provided by a designated gatekeeper. To be designated as a gatekeeper, a provider must meet three qualifying requirements,[7] namely the provider must:

(1) have a significant impact on the internal market;
(2) operate a core platform service which serves as an important gateway for business users to reach end users; and
(3) enjoy an entrenched and durable position in its operations.

[6] See Recitals (3) (referring to reduced contestability) and (4) (referring to the risk of serious imbalances in bargaining power and of unfair practices and conditions for business users, as well as end users of core platform services) DMA.

[7] An undertaking is presumed to satisfy these qualitative conditions if it meets the quantitative thresholds laid down in Art. 3(2) DMA (e.g. the core platform service must have at least 45 million monthly active users).

Until today, no provider of cloud computing services has been designated as a gatekeeper.[8] As pointed out by some experts [28], cloud computing services in general do not easily fit the logic of the DMA. The DMA targets intermediation services that intermediate between business users and end users, but cloud computing in general lacks multi-sidedness (i.e. does not act as an "important gateway for business users to reach end users"). This is particularly true in the case of a telco cloud, which solely hosts the core network or the radio network of a mobile network (as explained in Section 1.1). Therefore, a telco cloud in no way intermediates between business users and end users, but provides tools and functions for the MNO to efficiently manage its network.

While it is highly unlikely that, under the current DMA, a provider of a telco cloud can be designated as a gatekeeper, the Commission is empowered by Art. 3(7) DMA to adjust the methodology for the designation of gatekeepers. Hence, in the case this happens in the future, it is necessary to look closer at the obligations attached to the gatekeeper status.

Many of the DMA obligations are tailored to the specific services, in relation to which a company was designated as a gatekeeper. Obligations related specifically to cloud computing services are few. Under Art. 5(2) DMA, a gatekeeper must obtain user consent before combining personal data from its core services with other personal data. Under Art. 5(8) DMA, a gatekeeper is prohibited from requiring business users or end users to subscribe to any core platform services offered by a gatekeeper as a precondition for using its cloud services. Under Art. 6(2) DMA, a gatekeeper is prohibited from using business user data to compete against those business users. Under Art. 6(9) DMA, a gatekeeper is obliged to provide end users with effective data portability. Under Art. 6(10) DMA, a gatekeeper is obliged to provide business users with real-time access to data provided for or generated in the context of the use of the relevant core platform service.

In the context of a telco cloud, only three of these obligations are relevant, namely those that refer to business users. This is because telco clouds are used by telecommunications providers that are business users or, as per Art. 2(21) DMA, "legal person acting in a commercial or professional capacity using core platform services for the purpose of or in the course of providing goods or services to end users". Therefore, the obligation to ensure effective data portability does not apply to the telco cloud. All of the gatekeeper's obligations in relation to business users aim to increase competition and contestability of the market, with an underlying assumption that the gatekeeper will be trying to undermine them. Therefore, the prohibition of bundling cloud computing with other core platform services aims to reduce a potential lock-in. The prohibition to use business data of a business user to compete against this business user and the obligation of provision of real-time access to data should increase the business users' capacity to compete and level the playing field (both in relation to the gatekeeper).

In the context of the telco cloud, none of these obligations seems relevant or contributing to the solution of the issues of digital sovereignty and interoperability. This is because, firstly, they target market failures that do not exist in a telco cloud and, secondly, MNOs and various providers in the supply chain are not active on the same market.

Cloud computing under the Data Act

By contrast to the DMA, the DA applies to all cloud computing providers. Chapter VI DA aims to facilitate effective switching between providers of cloud computing services, and Chapter VIII DA – interoperability of cloud computing services, including when using several such services in parallel (i.e. multi-cloud).

[8] For the updated list of designated gatekeepers, please see: https://digital-markets-act.ec.europa.eu/gatekeepers_en.

The DA provisions on interoperability are very limited and do not seem to be conceptualised to be used in the context of a telco cloud.

The term "interoperability" is defined by the DA as "the ability of two or more data spaces or communication networks, systems, connected products, applications, data processing services or components to exchange and use data in order to perform their functions" (Art. 2(40) DA). As becomes clear from this definition, interoperability is limited to the use of data, which is only a small aspect of interoperability and, arguably, less relevant for a telco (multi-)cloud from the perspective of a telecommunications provider that also needs technical interoperability. In the cloud computing context, technical interoperability means the "capability of public clouds, private clouds, and any other systems in the enterprise to understand each other's application and service interfaces, configuration, forms of authentication and authorization, data formats etc. in order to cooperate and interoperate with each other" [37]. The DA does not seem to fully account for such technical interoperability. In addition, depending on the cloud service model (i.e. IaaS, PaaS or SaaS), the meaning of interoperability changes. For instance, IaaS and PaaS may need interoperable interfaces or APIs so that virtualisation platforms management can operate between different providers and the customer can migrate workloads between them, whereas in SaaS compatibility of data formats and protocols may suffice [30]. These nuances are also not captured by the DA.

The substantive DA provisions on interoperability in multi-cloud are the same as the DA provisions on switching, and the former shall apply to interoperability *mutatis mutandis*. Below we discuss the relevant switching provisions, and whether and how they may/can fit interoperability for telco multi-cloud.

Overview of main obligations in the context of multi-cloud use

Under Art. 23 DA, providers of cloud computing shall take a number of measures to enable their customers to switch between services of the same type. In this paper, we leave out the discussion of legal requirements related to contractual terms (e.g. the right to conclude new contracts, contractual transparency, content of contracts) and switching charges and focus only substantive obligations of cloud providers related to multi-cloud use and interoperability.

Cloud providers shall refrain from inhibiting their customers from (Art. 23 (c), (d) and (e) DA):

1. porting customer's exportable data and digital assets,
2. achieving functional equivalence in the use of the new cloud service of the same service type, and
3. unbundling IaaS from other cloud services.

Art. 24 DA states that the above obligations apply only to the source cloud provider in the context of switching. However, in the context of the multi-cloud use, all cloud providers are simultaneously source and destination cloud providers, hence these obligations apply to all of them.

Below we discuss each of the three obligations one by one.

Porting of customer's exportable data and digital assets

Porting is not defined by the Data Act, but based on the context it means the possibility for the cloud customer to freely move its data and digital assets between different clouds (e.g. Art. 23(c) DA). While the definition of data is a standard one,[9] digital assets are understood as "elements in digital form, including applications, for which the customer has the right of use, independently from the contractual relationship with the data processing service it intends to switch from" (Art. 2(32) DA). Recital 83 DA further explains

[9] Data means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording (Art. 2(1) DA).

that digital assets also include “metadata related to the configuration of settings, security, and access and control rights management, and other elements such as manifestations of virtualisation technologies, including virtual machines and containers”. The definition of digital assets as explicated in the recital could therefore cover containers or CNFs, which makes porting relevant for the multi-cloud use. For telcos using several clouds in parallel, the possibility to port data between different telco clouds is irrelevant as the actual data will be processed at a much higher layer, to which telco companies are unlikely to have access. However, porting of digital assets in the sense of running the same CNFs on two or more clouds may be a possible scenario, although we have not encountered it in practice during our research. Currently, MNOs run different CNFs on different clouds for the same network. However, in the future there may be a hypothetical scenario of running the same CNFs on different clouds in parallel.

Achieving functional equivalence

The source cloud provider shall not inhibit its customer from achieving functional equivalence in the use of the new cloud service of the same service type. Functional equivalence means re-establishing, on the basis of the customer’s exportable data and digital assets, a minimum level of functionality in the environment of a new cloud service of the same service type after switching, where the destination cloud service delivers a materially comparable outcome in response to the same input for shared features supplied to the customer (Art. 2(37) DA). Recital 86 DA explains that cloud providers “can only be expected to facilitate functional equivalence for the features that both the source and destination data processing services offer independently”.

According to Art. 30(1) DA, for IaaS providers there is an obligation to facilitate functional equivalence, which means taking all reasonable measures in their power that the customer achieves functional equivalence upon switching to the new provider. However, in practice in the context of the telco cloud, this provision is meaningless because, as shown Section 3.2, the IaaS interface is not used at all. The IaaS seems to lose significance in the telecom sector as the trend goes to using containers without virtual machines on bare metal. In particular, the DA suggests that IaaS providers in the context of multi-cloud use are obliged to facilitate the achievement of functional equivalence for their customers during such use, but only as long as this pertains to the use of other IaaS. In other words, this obligation does not apply to an IaaS provider to help achieving functional equivalence with a PaaS running on top of this IaaS (i.e. vertical functional equivalence). However, according to our deployment models for telco clouds in Section 3.2, this is one of the scenarios for telcos.

More general question can be asked with regard to achieving functional equivalence: to what degree the cloud services in the multi-cloud use are of the same service type. Art. 2(9) DA defines same service type as a “set of data processing services that share the same primary objective, data processing service model and main functionalities”. Recital 81 DA further explains that there are three main service delivery models (i.e. IaaS, PaaS and SaaS), but cloud services can be also categorised in a more granular way based on their primary objective and main functionalities. The DA does not define or explain what constitutes a “primary objective” or “main functionality” in this context. This means that whether two or more cloud services are “same service types” is to be determined on the case by case basis. For instance, can cloud services be considered “same service types” if they have different service delivery models or if a part of cloud services consistently lies beyond the IaaS layer and is clearly PaaS (as in the current deployment models)?

Unbundling IaaS from other cloud services, where technically feasible

The source cloud provider should not inhibit the customer from unbundling IaaS from other cloud services. This is regulated so that customers can make use of Art. 30(1) DA and achieve functional equivalence in IaaS when they switch cloud services. However, according to our research, the IaaS interface is not used in

the telco cloud, and it is not relevant in the environment with containers or Kubernetes on bare metal. Therefore, this provision is not relevant for the telco cloud in the multi-cloud use scenario.

Cloud providers, other than IaaS, must make open interfaces available to all customers and destination cloud providers (Art. 30(2) DA). They also must ensure compatibility with common specifications based on open interoperability specifications or harmonised standards (Art. 30(3) DA). All cloud providers must provider to customers an up-to-date online register with details of all data structures and formats as well as related standards and open interoperability specifications, in which the exportable data are available. If common specifications or harmonised standards do not exist, cloud providers must, at the request of the customer, export all exportable data in a structured, commonly used and machine-readable format (Art. 30(5) DA).

Cybersecurity measures for cloud

Cloud computing activities are subject to the general cybersecurity legislation, such as the NIS-2 Directive, which considers cloud computing a type of digital infrastructure and, therefore, a sector of high criticality, and the Cyber Resilience Act, which introduces special requirements to software, hardware and remote data processing solutions. Providers of cloud computing are, therefore, subject to enhanced risk management measures, must perform security tests and comply with strict reporting requirements of significant cybersecurity incidents. These legislations can be considered typical product and process security rules, applicable in various contexts.

The **NIS-2 Directive** does not restrict the choice of a supplier or service provider for sectors of high criticality a priori, but requires Member States to ensure that "essential and important entities"[10] take "appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services" (Art. 21(1) of the NIS-2 Directive). Such measures must ensure a level of security of network and information systems appropriate to the risks posed, taking into account – among other things – the degree of the entity's exposure to risks and likelihood and severity of incidents (Art. 21(1) of the NIS-2 Directive). Such measures must be based on an "all-hazards approach" aiming to protect network and information systems and the physical environment of those systems from incidents and include "supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers" (Art. 21(2) of the NIS-2 Directive).

Therefore, telecom providers are free to decide whether and which cloud services providers they use according to their internal risk management/ assessment procedures. However, Member States have the option to oblige telcos to use only specific cloud services providers that are certified under an EU cybersecurity certification scheme (Art. 24 of the NIS-2 Directive).

A dedicated certification scheme is currently still in preparation. The **European Cybersecurity Certification Scheme for Cloud Services (EUCS)** was commissioned by the European Commission to ENISA in 2019 as a way to strengthen and tighten cybersecurity standards for cloud services, which have been highly diverse across the EU Member States [32]. Although the draft EUCS was developed by ENISA in December 2020 [38], it has been revised several times since and is still far from formal adoption due to a long-standing discussion on the potential inclusion of sovereignty requirements in the EUCS.

[10] Providers of public electronic communications networks or publicly available electronic communications are considered essential entities as per Art. 3 (1) of the NIS-2 Directive.

The first EUCS draft of December 2020 [33] required cloud service providers to be transparent about the geographical location(s) of all system components, on which their customers' data is stored and processed, and the laws applicable to it. The 2020 draft stipulated that this information should be provided on the certificate.

However, the revised draft EUCS of May 2023[11] went much further and proposed additional requirements beyond traditional security controls. Analysts [39] observed that these new requirements were modelled on the French certification program SecNumCloud [40], which resulted in no non-French cloud provider being able to satisfy such requirements and to be certified. In particular, the EUCS divided the high assurance level into two cloud service evaluation levels (i.e. high and high+):

- CS-EL3 for "for cloud services that are designed to meet specific (exceeding level 'substantial') security requirements for mission-critical data and systems" and
- CS-EL4 for cloud services designed for "data of particular sensitivity that would present risks to society if breached", data "related to secrets protected by law" (e.g. national defence and security, government deliberations, etc.), and "the protection of privacy, to medical secrecy, and to trade secrets, which includes…information on commercial or industrial strategies…necessary for the accomplishment of essential State functions" [39].

The new Annex J attached to the 2023 draft EUCS contained four groups of detailed requirements ensuring [34]:

- Independence from non-EU law and that only EU law and national law of Member States apply to cloud services;
- Operation of the cloud service is in the EU. For CS-EL3 certification, this meant being transparent about the locations of data storage and processing, and management and support of their services, as well as offering at least one contractual option where all specified locations are in the EU. For CS-EL4 certification, all system components, on which the cloud service provider or its sub-service providers stored and processed data, had to be in the EU. Also management, monitoring and support had to be provided only from EU locations. Individual, precisely specified support activities were allowed from third countries only under exceptional circumstances;
- Only employees and business partners located in the EU or are monitored by a pre-screened EU resident employee can access customer data;
- Certification at the CS-EL4 (high+) level is only possible for providers with the registered head office and the global headquarters in the EU. Additionally, companies from third countries must not hold direct or indirect effective control over such a provider.

In March 2024, the third draft emerged,[12] however, without Annex J and the four groups of non-technical requirements [41]. The distinction into high and high+ assurance levels was also removed. The remaining 'sovereignty requirements' are limited to the obligation of transparency regarding the location of where customer data is stored and processed and to the obligation that cloud service providers must operate 'primarily' within EU law and law of EU Member States [34].

[11] The 2023 EUCS was leaked to news portal Politico. The text is not directly available anymore, but was widely discussed in various publications. The text is based on the reports of the time.

[12] The 2024 draft EUCS was also leaked. No final text of the EUCS has been published officially since the original first draft in 2020.

At the time of writing, the EUCS has not been adopted and, in fact, it remains to be seen whether and how the text may be changed in the future.

In the specific context of mobile communications, 5G/6G and cloud, the **EU Toolbox for 5G Security** [35] also comes into play. It was developed and adopted in 2020, after several EU institutions [42], [43], [44] recognised cybersecurity risks related to the dependency on an operator or operators from third countries. In identifying new risks, the EU Toolbox on 5G links economic developments to cybersecurity.

The EU Toolbox for 5G Security identified risks related to 5G supply chain (R4: dependency on any single supplier within individual networks or lack of diversity on nation-wide basis) and to modus operandi of main threat actors (R5: state interference through 5G supply chain). Accordingly, the Toolbox offers a set of strategic, technical and additional supporting actions. Of particular relevance to these risks are the following strategic measures:

- SM03 Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk - including necessary exclusions to effectively mitigate risks- for key assets;
- SM04 Controlling the use of Managed Service Providers and equipment suppliers' Third Line Support;
- SM05 Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies;
- SM07 Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU;
- SM08 Maintaining and building diversity and EU capacities in future network technologies.

Cloud computing is explicitly mentioned only in the context of one technical measure, namely the requirement to use cybersecurity certification for non-5G-specific ICT products and services. However, cloudification is more specifically addressed in the 'Report on the cybersecurity of Open RAN', which includes guidance on the Toolbox implementation [45].

List of Acronyms

3GPP	3rd Generation Partnership Project
AI	Artificial intelligence
AMF	Access management function
AR/VR	Augmented reality/ virtual reality
BEREC	Body of European Regulators of Electronic Communications
CaaS	Container as a Service
COTS	Commercial off the shelf
CNCF	Cloud Native Computing Foundation
CNF	Cloud-Native Network Function
CRM	Customer Relationship Management
CU	Centralised unit
DA	Data Act
DMA	Digital Markets Act
DU	Distributed unit
ENISA	European Union Agency for Cybersecurity
EPC	Evolved Packet Core
EU	European Union
EUCS	European Cybersecurity Certification Scheme for Cloud Services
FNS	Future Network Services
IaaS	Infrastructure as a Service
MNO	Mobile network operator
NFV	Network Function Virtualization
NIS	Network and information systems (directive)
NOC	Network Operations Centre
OEM	Original equipment manufacturer
PaaS	Platform as a Service
RU	Radio unit
SaaS	Software as a Service
SBA	Service-Based Architecture
SDN	Software-Defined Networking
SMF	Session management function

QoS	Quality of service
UPF	User plane function
VM	Virtual machine

List of Figures

References

[1] Tobias Bergtholdt, Christian Bartosch, Michael D. Breitenstein, Michael Steiger, and Rüdiger Schicht, „How Telcos Can Find the Right Balance in the Cloud," 28 February 2024. [Online]. Available: https://www.bcg.com/publications/2024/how-to-find-the-right-balance-in-the-telco-cloud.

[2] ACM, „Market Study Cloud services," 5 September 2022. [Online]. Available: https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf.

[3] D. Goovaerts, „Europe's cloud market poised for 24% growth," 28 July 2025. [Online]. Available: https://www.fierce-network.com/cloud/europes-cloud-market-poised-24-growth.

[4] De Nederlandsche Bank, „AFM and DNB warn of systemic risks in the financial sector from digital dependence," 20 October 2025. [Online]. Available: https://www.dnb.nl/en/general-news/press-release-2025/afm-and-dnb-warn-of-systemic-risks-in-the-financial-sector-from-digital-dependence/.

[5] M. Draghi, „The future of European competitiveness, Part B: In-depth analysis and recommendations," September 2024. [Online]. Available: https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf.

[6] Rijksoverheid, „Agenda Digitale Open Strategische Autonomie," 2023. [Online]. Available: https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa.

[7] European Commission, „How to master Europe's digital infrastructure needs? White Paper, COM(2024) 81," 21 February 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs.

[8] Stefan Rommer, Peter Hedman, Magnus Olsson, Lars Frid, Shabnam Sultana and Catherine Mulligan, 5G Core Networks, Academic Press, 2019.

[9] Massimo Villari, Ivona Brandic and Francesco Tusa, Achieving Federated and Self-Manageable Cloud Infrastructures: Theory and Practice, Business Science Reference, 2012.

[10] Google, „What are the different types of cloud computing?," [Online]. Available: https://cloud.google.com/discover/types-of-cloud-computing.

[11] Microsoft, „What are public, private, and hybrid clouds?," [Online]. Available: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds.

[12] S. Lean, „Cloud Terminology Explained," 19 October 2020. [Online]. Available: https://www.techielass.com/cloud-terminology-explained/.

[13] Google, „PaaS vs. IaaS vs. SaaS vs. CaaS: How are they different?," [Online]. Available: https://cloud.google.com/learn/paas-vs-iaas-vs-saas.

[14] I. Morris, „Telefónica to go deeper into public cloud after AWS 5G core fix," 24 March 2025. [Online]. Available: https://www.lightreading.com/mobile-core/telef-nica-to-go-deeper-into-public-cloud-after-aws-5G-core-fix.

[15] Nokia, „Nokia and Red Hat Announce Partnership for New Best-in-Class Telecommunications Solutions Based on Red Hat Infrastructure Platforms and Nokia's Core Network Applications," 29 June 2023. [Online]. Available: https://www.nokia.com/newsroom/nokia-and-red-hat-announce-partnership-for-new-best-in-class-telecommunications-solutions-based-on-red-hat-infrastructure-platforms-and-nokias-core-network-applications/.

[16] Microsoft, „What is Azure Private 5G Core?," 13 January 2025. [Online]. Available: https://learn.microsoft.com/nl-nl/previous-versions/azure/private-5g-core/private-5g-core-overview.

[17] „Linux CNCF," [Online]. Available: https://www.cncf.io/.

[18] „Sylva Project," [Online]. Available: https://sylvaproject.org/.

[19] „Project Anuket," [Online]. Available: https://anuket.io/.

[20] „O-RAN Alliance," [Online]. Available: https://www.o-ran.org/.

[21] „AI-RAN Alliance," [Online]. Available: https://ai-ran.org/.

[22] BEREC, „Report on the 5G Ecosystem, BoR(22) 144," 6 October 2022. [Online]. Available: https://www.berec.europa.eu/system/files/2022-10/BEREC%20BoR%20%2822%29%20144%20Report%20on%20the%205G%20Ecosystem.pdf.

[23] BEREC, „Report on Cloud and Edge Computing, BoR(24) 52," March 2024. [Online]. Available: https://www.berec.europa.eu/system/files/2024-03/BoR%20%2824%29%2052_Draft_Cloud_Report.pdf.

[24] Francesca Bria, Paul Timmers and Fausto Gernone, „EuroStack - A European Alternative for Digital Sovereignty," 13 February 2025. [Online]. Available: https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty.

[25] European Commission, „Commission approves up to €1.2 billion of State aid by seven Member States for an Important Project of Common European Interest in cloud and edge computing technologies," 5 December 2023. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6246.

[26] European Commission, „AI Continent – new cloud and AI development act," 9 April 2025. [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14628-AI-Continent-new-cloud-and-AI-development-act_en.

[27] „Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, OJ L 265, 12.10.2022," [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng.

[28] Konstantina Bania and Damien Geradin, „The regulation of cloud computing: why the European Union failed to get it right," *Information & Communications Technology Law,* pp. 99-113, 2024.

[29] „Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828, OJ L, 2023/2854, 22.12.2023," [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng.

[30] Sean Ennis and Ben Evans, „Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence," *SSRN,* 2024.

[31] „Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union," [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[32] European Commission, „Towards a more secure and trusted cloud in Europe," 9 December 2019. [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/towards-more-secure-and-trusted-cloud-europe.

[33] ENISA, „EUCS – Cloud Services Scheme," December 2020. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/publications/EUCS%20%E2%80%93%20Cloud%20Service%20candidate%20cybersecurity%20certification%20scheme.pdf.

[34] A. H. Philipp Eckhardt, „EU Cloud Certification at an Impasse: (Escape) routes leading to a resilient cloud policy in the EU," 25 April 2025. [Online]. Available: https://www.cep.eu/fileadmin/user_upload/cep.eu/cepItalia/cepInput_EU_Cloud_Certification_at_an_Impasse.pdf.

[35] NIS Cooperation Group, „Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures," 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[36] US NIST, „The NIST Definition of Cloud Computing," September 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[37] Niamh Gleeson and Ian Walden, „Cloud Computing, Standards, and the Law," in *Cloud Computing Law*, OUP, 2021.

[38] ENISA, „Cloud Certification Scheme: Building Trusted Cloud Services Across Europe," 20 December 2020. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme.

[39] Kenneth Propp, Peter Swire and Josh Fox, „Oceans Apart: The EU and US Cybersecurity Certification Standards for Cloud Services," 11 July 2023. [Online]. Available: https://www.crossborderdataforum.org/oceans-apart-the-eu-and-us-cybersecurity-certification-standards-for-cloud-services/.

[40] ANSSI, „SecNumCloud pour les fournisseurs de services Cloud: Pourquoi et comment être qualifié SecNumCloud?," 29 September 2023. [Online]. Available: https://cyber.gouv.fr/secnumcloud-pour-les-fournisseurs-de-services-cloud.

[41] J. Rone, „No EU cloud in sight: How diverging member states' preferences get in the way of achieving EU cloud sovereignty," 6 August 2024. [Online]. Available: https://blogs.lse.ac.uk/medialse/2024/08/06/all-bark-and-no-bite-how-diverging-member-states-preferences-go-in-the-way-of-achieving-eu-cloud-sovereignty/..

[42] „Commission Recommendation (EU) 2019/534 of 26 March 2019 on Cybersecurity of 5G networks, OJ L 88," [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534.

[43] „Council Conclusions on the significance of 5G to the European economy and the need to mitigate security risks linked to 5G 3 December, 2019 14517/19," [Online]. Available: https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.

[44] „European Parliament resolution of 12 March 2019 on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them (2019/2575(RSP)," [Online]. Available: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.pdf?redirect.

[45] NIS Cooperation Group, „Report on the cybersecurity of Open RAN," 11 May 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks.

[46] IDATE and Schuman Associates, „5G Observatory report 2025," 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/5g-observatory-2025.

[47] NIS Cooperation Group, „Second report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity," June 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.

[48] European Commission, „Commission launches market investigations on cloud computing services under the Digital Markets Act," 18 November 2025. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2717.