WHITE PAPER

analysys mason

Digitalizing 5G: elastic, programmable and secure

Caroline Gabriel

JULY 2018

Contents

List of figures

1. Executive summary – 5G Network & Operations

Evolving from today's Communications Service Provider (CSP) to tomorrow's Digital Service Provider (DSP) is not an option, it is a necessity.

A CSP focuses mainly on the connectivity to enable the services of others. But to reap the full commercial benefits of new networks, in the era of 5G and dense fiber, many will become DSPs, providers of a wide range of digital and online services from content to payments, delivered directly to the device. Service providers will have crucial decisions to make about their core business models. While some will choose to focus mainly on providing connectivity to support digital partners, many will aim to move up the value chain and offer a richer set of digital services.

Whatever the business decision, it will be essential to undergo digital transformation. This means supporting online, mobile services and customer interactions, enabled by a new OSS/BSS platform which is virtualized and based on microservices and the cloud. This, in turn, requires the CSP to invest in an entirely new kind of network - one that will be elastic, programmable and highly secure - in order to adapt to a wide range of service models.

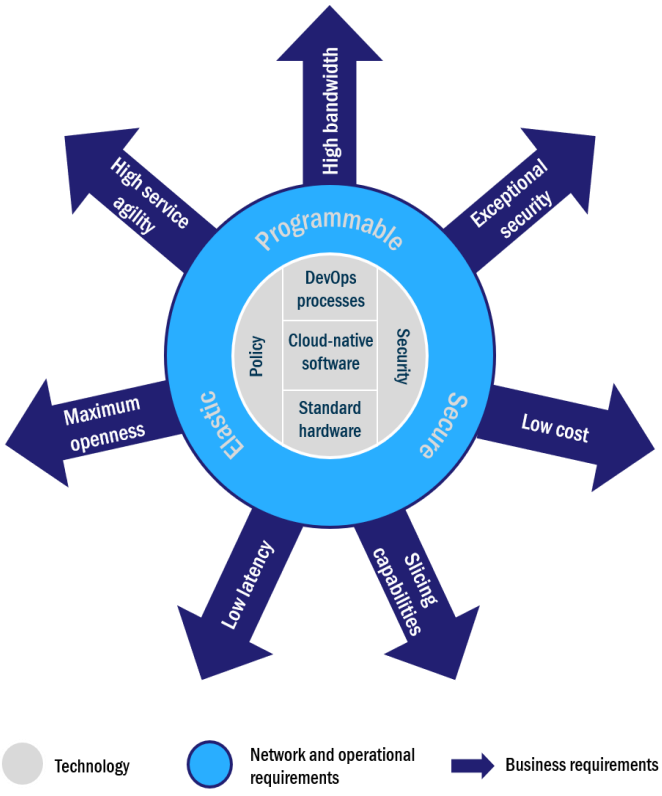


Figure 1: Seemingly incompatible requirements of 5G network and operations [Source: Analysys Mason, 2018]

Becoming a DSP entails resolving many apparent conflicts. DSPs need to achieve high levels of value and differentiation, at the same time as very low-cost operations, in order to achieve the agility to compete effectively. The network, similarly, has to reconcile demands that appear directly opposed to one another. It must be very open, but also extremely secure. It must be fully virtualized, but support tight integration of physical and virtual. It must enable extreme automation, but also be highly responsive to changing demands.

The service characteristics the network of the 5G era must support also appear divergent, and even incompatible: high bandwidth alongside ultra-low-cost, low-volume connectivity, as well as ultra-low-latency services; billions of open interface points to customers, things, and trading partners, but with exceptional security. To meet all these requirements will require a revolution in the underlying technology of the network and the accompanying operations functions.

This integrated network of the future will be aided by new 5G standards, but they will not be enough on their own. Indeed, a whole new platform will be essential to make sense of investment in 5G.

The end result should be a network that can support a wide range of digital services, including those in the Internet of Things (IoT). This network will represent a radical change in architecture, management, skills and operator culture. It will have absorbed and automated most of the functions formerly served by external operations support systems (OSS), providing an extremely automated, flexible Digital Network.

Many of the technologies which will help to achieve this goal have been discussed at over recent years, but are now starting to be commercialized in the telecoms market:

- Use of cloud computing and storage, at any appropriate location in the network from core to edge.
- A maximally virtualized network infrastructure, which can draw flexibly on many resources including 5G radios and fiber (FTTx). This will make use of commercial off-the-shelf (COTS) hardware where appropriate, but will also require specialized processors for functions like baseband processing.
- Use of new web-scale software techniques such as Cloud Native Software Architecture, DevOps processes, Continuous Integration/Continuous Deployment (CI/CD) delivery mechanisms.
- AI/ML-based approaches for autonomous actions in the network which can anticipate problems and predict 'unhealthy' network states. AI/ML is becoming important for the management of quality of service (QoS), network slices and security.

The combination of these technologies with emerging open frameworks will support a set of foundational operational requirements for:

- Programmability of a sliceable 5G network to provide service agility and support of the multiple, often incompatible business requirements.
- Automated elasticity of the network and operational functions to meet growing and short-term service needs effectively and inexpensively.
- A ubiquitous security architecture.

All these will require functionality built into the (virtualized and physical) network and into the operations software, under end-to-end business control. Planning and implementing the required major network transitions will require expertise in network technologies, BSS, OSS, and new software technologies. Some CSPs may grow that expertise themselves. Most will work with vendors and systems integrators which understand the whole picture.

For many CSPs, the most impactful result of this transformation will be the enablement of network slicing, which will support a wide variety of new business models and revenue streams. A fully agile, sliced network will be an ongoing transformation process. The elastic, programmable, secure network is not an end goal – it is the starting point for an ongoing process of business transformation, an architecture flexible enough to take advantage of many new technologies and processes as those emerge.

2. 5G business transformation imperatives

Many CSPs are starting to devise digital transformation strategies. The transformation path will be unique to each CSP, but will share some common characteristics. In Analysys Mason's definition, the path is defined by a digital vision of the CSP's business and network; it provides both near-term and long-term value; it is customer-centric in design; and it is implemented using fast iteration approaches. Digital transformation addresses three areas: digital services (moving beyond connectivity); digital experience (direct access to applications and customer service via the smartphone interface); and digital agility of business and network operations (a virtualized, microservices-based platform designed to respond quickly to customers' needs).

Therefore, CSPs which decide to become DSPs aspire to digitalize their service offerings, and that requires a radical rethink of the network and its operations, both 'in the front' and 'at the back'. The principles of elasticity, programmability and security must be instilled in all three main layers of the network – BSS (business support systems); OSS (operational support systems); and access, core and transport – to address the diverse requirements of the digital business.

The 'front' is primarily the domain of the BSS of today, providing a set of digitized low-cost channels and a modern, digital experience to consumers, enterprise customers, suppliers and resellers. We call the next-generation BSS the 'Digital Business Platform' (DBP)[1] . This will be built on cloud-native technology and include digitized support for 'things' as they become consumers of CSPs' services in an IoT world.

The front consists of the OSS and the network itself (access, core and transport). Increasingly, the lines will blur between these as the OSS evolves into an orchestration layer and works very closely with the network, to provide service agility, operational flexibility, and cost savings via massive automation of network operations (see Figure 2).

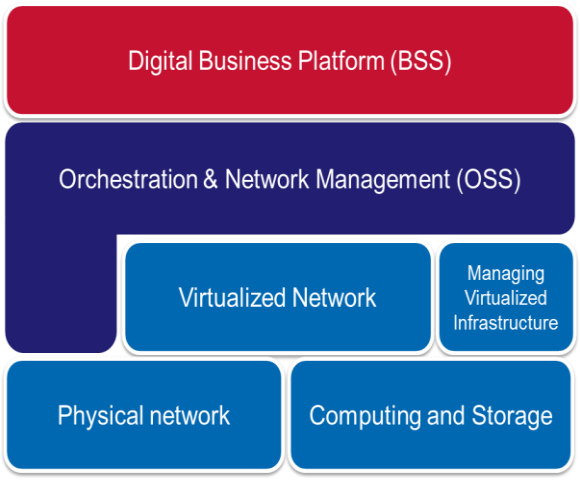


Figure 2: The next generation BSS, OSS, and network will be layered, much as today, but highly automated [Source: Analysys Mason, 2018]

The network will be transformed by a new generation of cloud-native software orchestrated by the next generation OSS, and running in private or hybrid clouds, providing many of the (virtualized) functions formerly supported by specialized hardware.

This is about far more than efficiencies, though those are inherent in the new architecture. Future BSS and OSS are software platforms that become the business, not support the business. Automation and artificial intelligence agents will perform most of the day-to-day functions, with people performing the governance functions: monitoring, configuring, and changing the platforms while ensuring the security for its customers.

[1] Mortensen, Mark H and Abraham, John, http: //www.analysysmason.com/Research/Content/Short-reports/digital-business-platforms-RMA15/#06%200ctober%202017

Orchestration and network management

The conventional OSS will evolve into the orchestration and network management layer, working increasingly intimately with the network[2] as a curated set of disaggregated software components from which a CSP's customer-facing services and operations will be composed. It needs to look like a software system, but will act as a platform with open and extensible properties.

This layer will provide a common set of self-managing services[3] which provide function to one another, using cloud-native architecture for resilience and deployment flexibility. Model-driven, orchestrated processes automate the definition, discovery, composition, instantiation, execution and lifecycle management of network services. The network function, IT, lifecycle management and infrastructure components required for each service are automatically assembled.

The CSPs will source these services from different suppliers, including vendors and open source communities. CSPs will differentiate themselves by curating their own sets of services and extending and changing these over time to meet market needs.

In future, this approach will enable the creation of network slices, which will be granular and dynamic, each one optimized for an individual service or customer, enabling radical new business models for CSPs (see Chapter 4).

The access network

One of the challenges for the new virtualized network is that elements of the access network clearly remain physical. Radios, antennas and fibers are obvious examples, and different operators will draw different boundaries between virtual and physical. Whatever those architectural decisions, the physical components still need to be orchestrated by the same software in order to deliver the maximum performance and flexibility.

This will allow physical resources to be harnessed far more flexibly. Software will enhance functionality and allocate resources where they are most valuable, to an increasing degree. The best example is the virtualized RAN (vRAN), in which physical radio/antennas take instructions from fully virtualized basebands, running on cloud platforms.

This becomes critical in network slicing, where a virtual slice must be carved end-to-end from access to application layers. In the new agile network, all elements can be treated in the same way by the orchestrator, allowing for far closer, and more dynamic, interworking between radio and fiber, physical and virtual. The 5G New Radio is a particularly important enabler in this new network because it has been optimized to support virtualized RAN and slicing in a standardized way, reducing the cost and risk of network transformation.

All of these software components will be based on the same software technology and methodology

All of these systems will be based on the evolution of today's leading-edge software technologies. Many have come from the web-scale companies and have been in use for over a decade, while some are just emerging, as shown in Figure 3.

[2] The combination of the next generation cloud-native OSS plus highly virtualized cloud-native network has been called a Digital Network & Operations Platform. See, Chappell, Caroline http://www.analysysmason.com/Research/Content/Short-reports/Defining-DNOP-5G-RMA16-RMA07-RMA18-RMA01-RMA02-RMA04/

[3] These 'services' are defined as domain-centric software components built using service-based or microservice design patterns.

Figure 3: Software technologies for next generation 5G operations [Source: Analysys Mason, 2018]

Technology	Description	Maturity
Cloud-native architecture	A modern software architecture where internal APIs replace the three-tiered client-server architecture, creating a set of microservices for internal and external use and carrying the data in a journaled manner. It is more compute-intensive, but provides far greater flexibility than existing approaches. Everything becomes a service that is available internally and (with proper security) can be made available as an external service.	Proven in FANGA[4] applications.
DevOps	An extension of the 'agile' software development methodology to include the post-implementation 'operations' phase where developers move to support the operational deployment phase, not just the build and test phase of the project.	Agile has been proven. DevOps is looking good, but requires extensive retraining.
Continuous Integration/ Continuous Delivery (CI/CD)	A software delivery methodology that, coupled with cloud-native architecture and DevOps, provides a continuous stream of bug fixes and feature evolution. It obviates the need for lengthy integration and includes highly automated regression testing.	In use in FANGA. Being trialled in many CSPs today.
Cloud deployment	Deployment of the software on modern, virtualized data center infrastructure. This could be on-premise, hybrid, or public cloud. It also includes managed services and software-as-a-service (SaaS) deployments on private clouds.	Proven in enterprise. Moving quickly in CSPs.
Artificial intelligence	Encompassing a wide range of techniques, from well-understood big data analytics and robotic mechanization to evolving deep search and machine learning through leading-edge natural language interfaces, cognitive computing and neural networks.	Evolving very quickly in all industries.

[4] FANGA – Facebook, Amazon, Netflix, Google, and Apple

3. The elastic digital network must resolve conflicting demands of 5G markets

It is important to remember that the new digital network is not being implemented solely to support current business models more efficiently. The main justification for this enormous upheaval, for most CSPs, will be the ability to operate in an entirely new way, enabling new revenues and service models. Many of the early examples of this transformation come from the fixed-line world – Telstra's Programmable Network, for instance, or AT&T's Domain 2.0 program. The new capabilities of the 5G core and access networks will put similar change more firmly within the grasp of mobile operators.

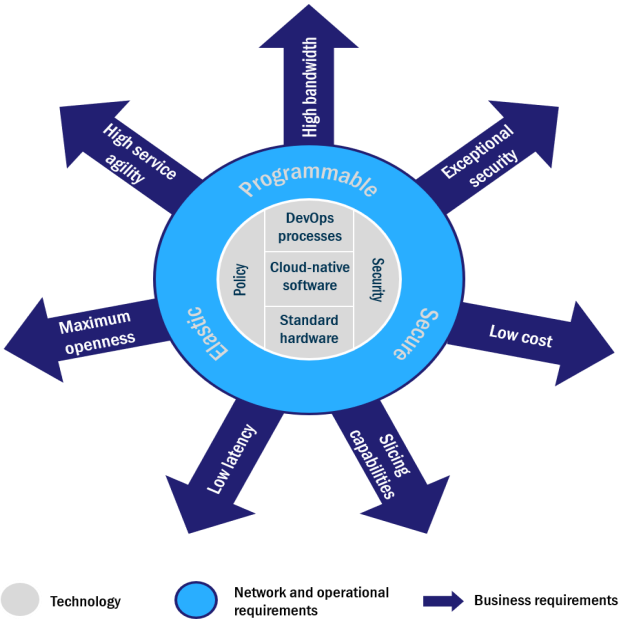
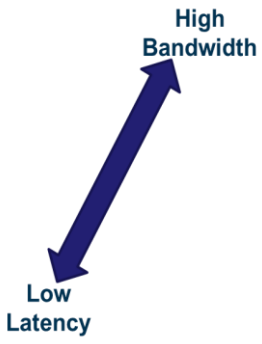


Figure 4: Seemingly incompatible requirements of 5G network and operations [Source: Analysys Mason, 2018]

However, this reinvention of the network and the business requires CSPs to resolve several apparent conflicts. To achieve maximum agility, the CSP's network will have to reconcile demands that appear directly opposed to one another. It must be very open, but also extremely secure. It must be highly automated, but able to respond to constant changes in demand. It must support many connectivity types in parallel - high bandwidth, ultra-low cost, low volume, ultra-low latency. It must have billions of open interface points to customers, connected objects and trading partners, but with exceptional security.

Resolving these conflicts means harnessing the software technologies outlined above in the most agile way. That will help remove the compromises between multiple requirements, which have always been a challenge in shared networks such as cellular, and which, without a new approach, would threaten to weaken the 5G model severely.

High bandwidth but low latency



Original packetized networks provided a single set of shared resources with the same service characteristics and QoS – all packets were created and treated equally. With the evolution to multiprotocol systems, individual services could traverse the routers and links with special characteristics and they would be treated differently with regards to queueing priority, backup and recovery, and other characteristics. But the devices involved had to do the best job they could with the resources available. Too many high-priority services could degrade their QoS, for instance. Packet networks have a challenge with simultaneous high-bandwidth and low-latency requirements, in particular[5]. Network slicing seeks to ameliorate the situation by assigning resources to a particular service or user, so its traffic can be

[5] Although theoretically, "all" one would have to do is have strong admission control, a set of very underloaded, low-latency routers, well-underloaded links, and more than sufficient backup to keep congestion from ever happening. This would be very expensive.

routed with the optimal characteristics for that service, such as ultra-low latency. How many slices there will be and how the hierarchies of slices will be managed is still a major point of discussion.

High service agility but low cost

Flexibility usually competes against low cost. The 5G network will critically require the ability to test, deploy, support, scale and, eventually, decommission, new services - all with great speed. But it must do so at a low cost, both in capex and opex. The use of web-scale techniques such as DevOps, as outlined above, is critical to achieving this balance.

Open but secure

The 5G network must be very open – providing communications and digital services to the DSP's customers and partners at the network endpoints. But it must also secure the network against malfeasance as well as errors from partners and customers. It also will provide operations functions under the direct control of its employees, automated agents, and partners that, without proper security could open the network to vast abuse. A total end-to-end view of the security is paramount, along with forensic and control functions.

3.1 Linking the business requirements to the Network and Operational requirements

Figure 5 shows the linkage between the business requirements and the network and operational requirements. The key to meeting the requirements is to provide not only elasticity of the resources and programmability of the functions, but also security as an in-built end-to-end function. This combination will support next generation technical and commercial approaches such as network slicing.

Figure 4: Linking 5G network business requirements with network and operational capabilities [Source: Analysys Mason, 2018]

	Elastic	Programmable	Secure
High Service Agility	Support successful new services growth, with the investment curve matching the revenue curve. Implement a wide range of services with incompatible network requirements.	Quickly configure, test, implement and scale new services.	Provide security on 'Day-One' for new services, not as an add-on.
Low Cost	Just-in-time network capacity augmentation and decommissioning. Low-volume, occasional IoT traffic routed by cheapest path.	Highly generic hardware in distributed data center and customer premises. Specialized software spun up to meet the specific needs of a slice.	
Maximum Openness	Resource sizing and service characteristics under fine control by customers. Access control only to resources dedicated to customers and trading partners.	Portals to customers and trading partners for cooperative operations and services exposure for cooperative development.	Standard security functionality for virtual and physical elements, operations control functions, and users.
Exceptional Security	Access control and logging of behaviours of individual slices provides good forensics.	Intent-based programmability limits the control of insiders and outsiders.	Overall security architecture implemented in cooperation with standard security features in network elements and BSS and OSS applications.
Ultra-high Bandwidth	Using only the resources required when required, with little delay.	Can be reserved, auto-scaling (to limits), burst, etc. through software configuration, with controllable QoS.	
Low Latency	Uses specialised routing and elements, in just the right quantity, when required, with little delay.	Can combine low latency and high bandwidth (within limits) according to need. Low-latency slice can be engineered separately from normal ones, reducing costs.	

Elastic

The network must monitor itself and its utilization, automatically creating new virtualized resources to meet the demand for more capacity in any area. This will obviate the need for ordering specialized hardware ahead of the actual need in the network since these virtualized resources will automatically scale with demand. Only network elements that move photons or electrons will be physical and require the standard engineering work.

Programmable

The network must be highly adaptable to new services, behaviours, and technologies. This will require that it be 'programmable' through the deployment of new or modified microservices as well as intent-based and policy-based programming by the business and operational personnel. Monitoring and governance of the results will, of course, be required.

Secure

Without trusted security, the new architecture will be non-viable. In a survey of 68 mobile CSPs conducted by Analysys Mason in November 2017, security and privacy concerns emerged as the second most significant barrier (after cost) to starting 5G deployment before 2023.

The 5G network will have to deal with unprecedented challenges. It will be open to millions, eventually billions, of Internet-connected devices. For some services, it will operate in real time and with high availability requirements. It will be handling massive levels of signalling, which if poorly managed could create storms and outages. Embedded SIMs are often accompanied by 'bring your own identity' approaches. 5G will be relying on open protocols which have come from outside the 3GPP world, and in a virtualized environment, cannot rely on security baked into a dedicated hardware appliance. All these changes hold great business potential – provided they are secured, and meet ever-increasing expectations of security and privacy protection.

A holistic approach to security is therefore essential. An assembly of hard-coded solutions that are closed, unintegrated and monolithic, such as today's, will be unacceptable.

There is a need for an automated centralized management/orchestration function to collect and analyse feeds from different operational silos; detect anomalous traffic, identity and access privileges; and configure network changes in response. For ultra-reliable low-latency communications, (URLLC), there will need to be dedicated cloud security resources placed at the network edge (e.g. in the factory for a manufacturing automation service) to handle near-real time demands. The system needs a holistic view of the operator's security posture across physical and virtualized networks and IT infrastructure. It will take advantage of machine learning for anomalous behavior detection[6].

Security also needs to be proactive, not reactive, to potential threats. The centralized Security Operations Center, which must take its place with the Network Operations Center and Service Operations Center, must make use of active security: using policies to micro-segment the network, detect security posture changes and drive appropriate responses within micro-perimeters[7]. This will require centralized analysis, but distributed enforcement and response. For instance, security for synchronous processes like RAN signalling could be placed close to the access to keep any threats away from the user plane. However, it will be critical that it not be limited to just single response – it may require a more comprehensive, incident response process implemented across multiple operational domains.

In addition, there will be specific security requirements for different types of traffic, for instance when initiating ultra-low-latency communications. Slicing will help CSPs to map the type and level of security to the service requirements.

[6] E.g. with IoT/smartphone traffic – threat remediation/mitigation could be to influence PCRF to throttle bandwidth or reset devices.

[7] E.g. instantiate a honeypot to trap traffic or scale a resource etc.

4. Network slicing best demonstrates the business impact of the elastic, programmable, secure network

Overall network automation and agility, and comprehensive security, cannot be accomplished domain-by-domain, but must be done end-to-end. This will require a comprehensive view of:

- The load the devices attached to the network are presenting.
- The state of all the network endpoints (including any edge computing devices),
- The physical and virtual network elements, underlying computing and storage resources.
- The controlling and supporting software.

Information must be collected, analyzed and evaluated, and automated action taken in a closed-loop fashion for all but the most difficult issues encountered. These will be sent to the experts (automated and human) for evaluation and action.

Once achieved, this holistic, software-driven network can be the foundation of a far wider range of digital services and businesses than the conventional CSP network. Each slice can have its own connectivity characteristics, such as low latency for a manufacturing service, but will also draw on other resources, such as compute processing and storage, as required (e.g. a virtual reality slice would combine graphical processor capabilities with low-latency connectivity). However, this is not a stationary target. The service models will evolve, including applications we cannot currently foresee; and the network platform must adapt to this. That is the real significance of a network which is planned today to be fully agile and elastic – it will be able to adapt itself for new behaviors in future, without the DSP having to replace it and start again.

The best illustration of how this ever-evolving, agile approach will impact a DSP commercially is network slicing. Virtualization lays the foundations for a world in which applications will automatically navigate their optimal path end-to-end through a highly responsive network. They will call up virtual slices which will include the appropriate physical and software resources, and the optimal levels of security, QoS, latency and bandwidth, for that particular application. This will resolve the trade-offs inherent in having to support many types of traffic on a single network, as outlined in Chapter 3.

Over time, the architecture will evolve to support increasingly dynamic, on-demand and sometimes ephemeral slices. This has the potential to enable huge numbers of service providers, enterprises and applications, and so diversify the DSP's model dramatically. This goal will not be achieved overnight, and there are still technical and commercial debates about how many slices will be practicable or profitable. However, as the network and orchestration platforms evolve, so will the options available for the DSP to support a large variety of services and customers via slicing. In our view, there will be three main phases of network slicing.

- Phase 1 will use existing capabilities to support static, capacity-based slices and will focus primarily on efficiencies using improved automation.
- Phase 2 will support single-tenanted, service-specific slices for a wider variety of users than Phase 1. These slices will be created on a more dynamic basis by automated slice managers. They will draw on underlying physical network resources as well as virtual network functions.
- In Phase 3, the application itself will call up the physical and virtual resources it needs for an optimal end-to-end route.

The DSP can start expanding its revenues and reducing its costs in Phase 1, but the greater monetization potential lies in developing rich platforms to support differentiated capabilities in later phases, and in so doing, maximize the benefits of the investment in the elastic, programmable and secure network.

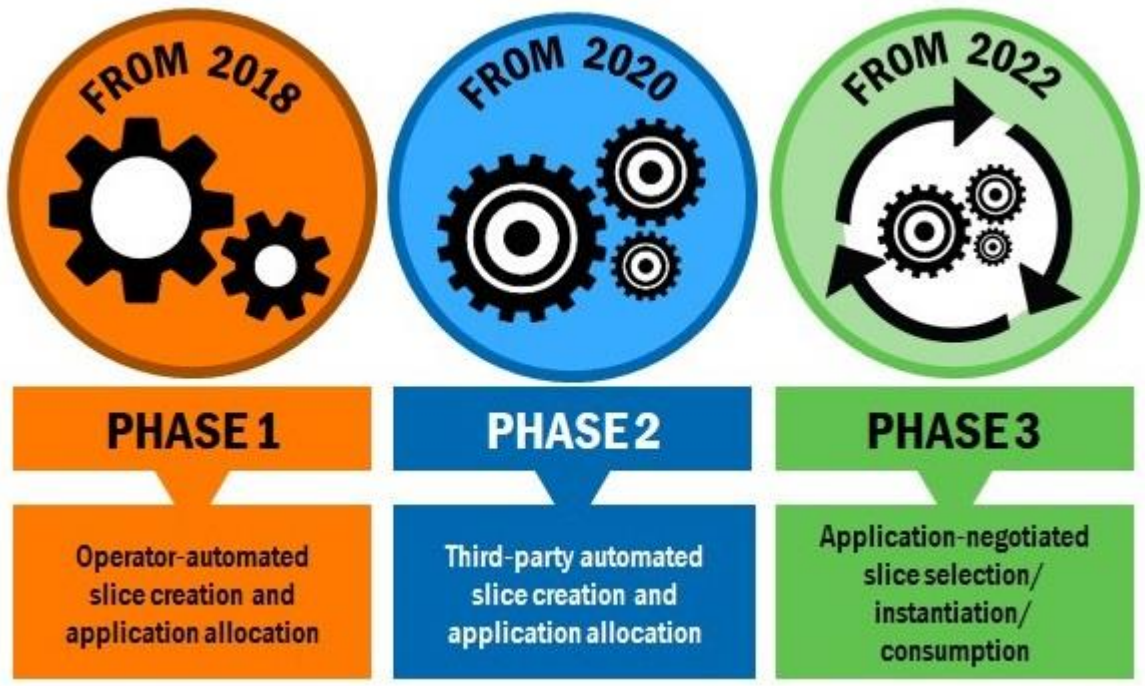


Figure 6. The network of the future will be sliced on different levels to support a wide range of service models and highly flexible resource usage [Source: Analysys Mason 2018].

5. Recommendations

The converged digital, fixed/mobile network of the future will be very different from today's capital and operationally intensive network. It will be software-driven and perform many of its functions automatically. But, to achieve that new network, and monetize it effectively, will require that CSPs wish to become DSPs. To do so they need to:

- Plan their future software-driven network and operations environment now, including plotting the evolution of current networks and operations systems to the new software technologies Accept that this is will be an ongoing process of change, so ensure that the framework is as open and flexible as possible to be able to adapt to unforeseen future opportunities.
- Make security of the network and services an intrinsic part of the technology and operational plans.
- Expand their skill sets to include the new software technologies such has cloud native and microservices architectures, as well adopt development and implementation methodologies of Continuous Integration/Continuous Deployment.
- Develop their own expertise, or work with vendors who have a comprehensive view of these new architectures and have experience in all areas of network, operations and business operations. These

will be needed as CSPs determine how to add value to the open source software components they will be using.

- Experiment with IoT market opportunities by enabling the network to support large numbers of devices with low bandwidth, but high reliability and security requirements. This will include URLLC (ultra-reliable low-latency communications) services.
- Identify new markets which could deliver increased revenues using 5G capabilities such as extreme bandwidth and low latency. Lay the foundations for network slicing now, so that all the new markets outlined above can be supported in parallel from a single, unified physical network and orchestration platform.

About the author

Caroline Gabriel (Senior Contributing Analyst) Caroline contributes to several Analysys Mason research programmes on topics related to mobile networks. She has been engaged in technology analysis, research and consulting for 30 years, and has focused entirely on mobile and wireless since 2002. Her focus is on critical issues and trends related to mobile and wireless infrastructure, particularly operator deployment intentions for 4G, 5G, cloud-RAN and other technologies.

Published by Analysys Mason Limited • Bush House • North West Wing • Aldwych • London • WC2B 4PJ • UK
Tel: +44 (0)20 7395 9000 • Email: research@analysysmason.com • www.analysysmason.com/research

Registered in England No. 5177472

Analysys Mason's consulting and research are uniquely positioned

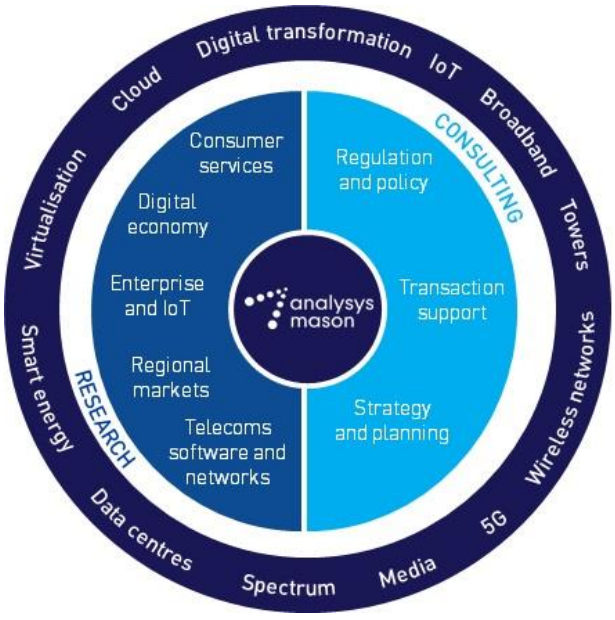
Analysys Mason is a trusted adviser on telecoms, technology and media. We work with our clients, including communications service providers (CSPs), regulators and end users to:

- design winning strategies that deliver measurable results
- make informed decisions based on market intelligence and analytical rigour
- develop innovative propositions to gain competitive advantage.

We have more than 220 staff in 13 offices and are respected worldwide for exceptional quality of work, independence and flexibility in responding to client needs. For 30 years, we have been helping clients in more than 100 countries to maximize their opportunities.

Consulting

- We deliver tangible benefits to clients across the telecoms industry: communications and digital service providers, vendors, financial and strategic investors, private equity and infrastructure funds, governments, regulators, broadcasters, and service and content providers.
- Our sector specialists understand the distinct local challenges facing clients, in addition to the wider effects of global forces.
- We are future-focused and help clients understand the challenges and opportunities that new technology brings.



Research

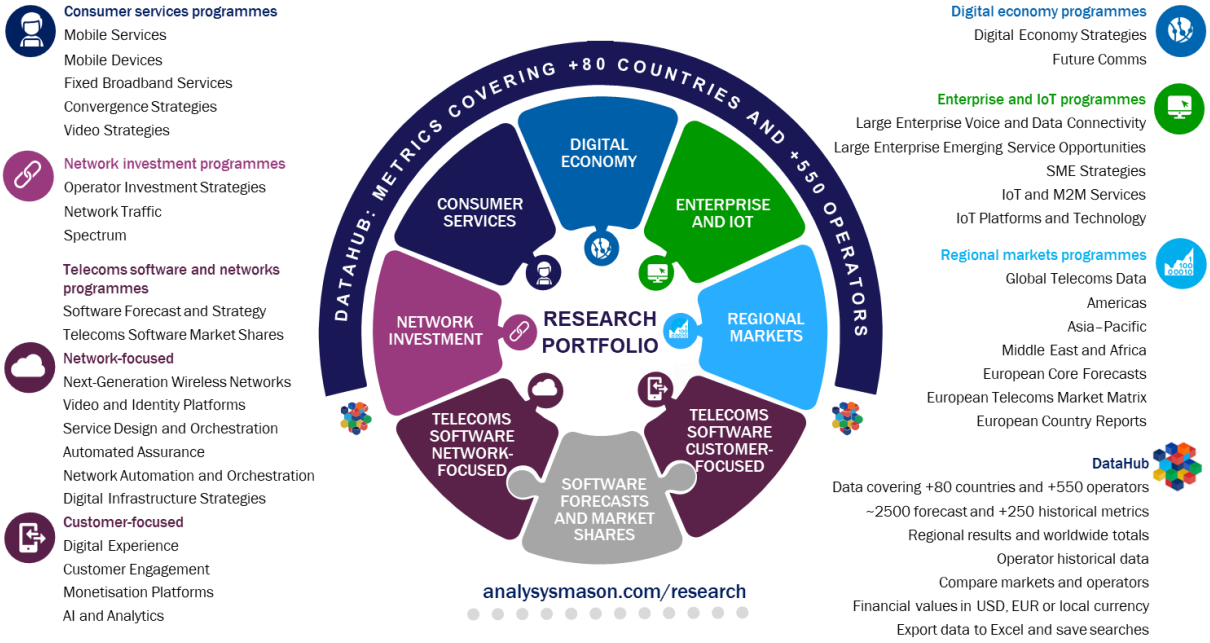
- Our dedicated team of analysts track and forecast the different services accessed by consumers and enterprises.
- We offer detailed insight into the software, infrastructure and technology delivering those services.
- Clients benefit from regular and timely intelligence, and direct access to analysts.

Research from Analysys Mason

We provide dedicated coverage of developments in the telecoms, media and technology (TMT) sectors, through a range of research programmes that focus on different services and regions of the world

The division consists of a specialised team of analysts, who provide dedicated coverage of TMT issues and trends. Our experts understand not only the complexities of the TMT sectors, but the unique challenges of companies, regulators and other stakeholders operating in such a dynamic industry.

Our subscription research programmes cover the following key areas.



Each subscription programme provides a combination of quantitative deliverables, including access to more than 3 million consumer and industry data points, as well as research articles and reports on emerging trends drawn from our library of research and consulting work.

Our custom research service offers in-depth, tailored analysis that addresses specific issues to meet your exact requirements

Alongside our standardized suite of research programmes, Analysys Mason's Custom Research team undertakes specialised, bespoke research projects for clients. The dedicated team offers tailored investigations and answers complex questions on markets, competitors and services with customised industry intelligence and insights.

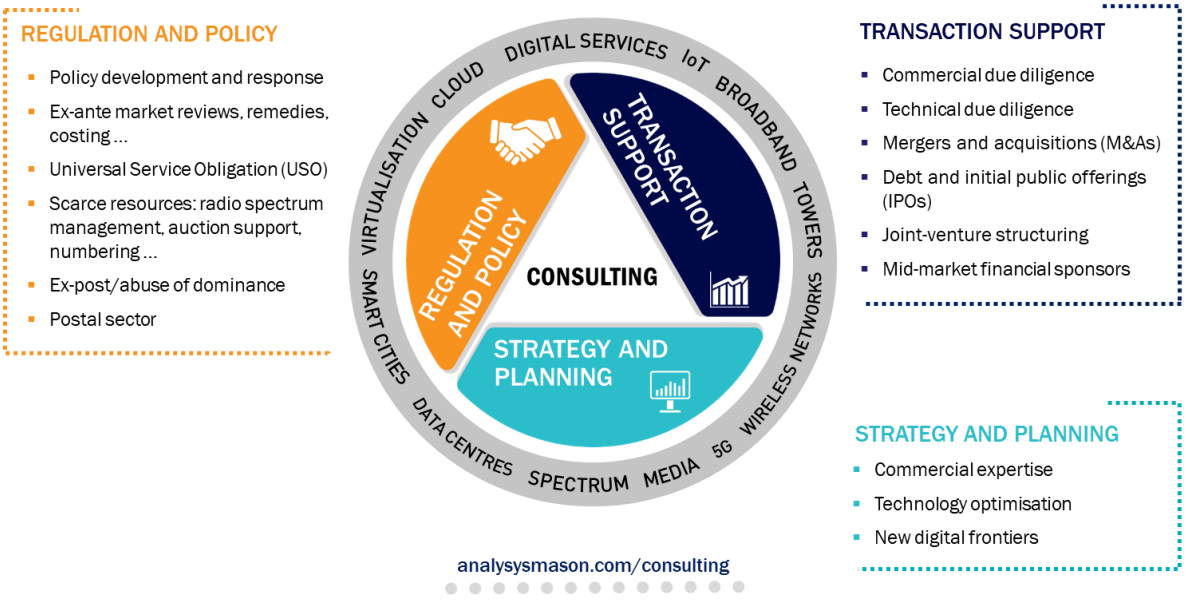
For more information about our research services, please visit www.analysysmason.com/research.

Consulting from Analysys Mason

For 30 years, our consultants have been bringing the benefits of applied intelligence to enable clients around the world to make the most of their opportunities

Our clients in the telecoms, media and technology (TMT) sectors operate in dynamic markets where change is constant. We help shape their understanding of the future so they can thrive in these demanding conditions. To do that, we have developed rigorous methodologies that deliver real results for clients around the world.

Our focus is exclusively on TMT. We advise clients on regulatory matters, help shape spectrum policy and develop spectrum strategy, support multi-billion dollar investments, advise on operational performance and develop new business strategies. Such projects result in a depth of knowledge and a range of expertise that sets us apart.



We look beyond the obvious to understand a situation from a client's perspective. Most importantly, we never forget that the point of consultancy is to provide appropriate and practical solutions. We help clients solve their most pressing problems, enabling them to go farther, faster and achieve their commercial objectives.

For more information about our consulting services, please visit www.analysysmason.com/consulting.