No. 108 / 4th quarter 2017

DIGIWORLD Economic Journal

COMMUNICATIONS
& STRATEGIES

The Sharing Economy: Myths and Realities

Edited by
Anders HENTEN, Denis LESCOP,
Jean Paul SIMON & Bruno SORIA

- Lobbying as Rhetorical Framing in the "Sharing Economy": a case study on the limits and crisis of the Evidence Based Policy Paradigm
- Platforms at the Heart of New Form of Labour
- The Rise and Fall of Take Eat Easy, or Why Markets are not Easy to Take in the Sharing Economy
- More generous for small favour? Exploring the Role of Monetary and Pro-Social Incentives of Daily Ride Sharing Using a Field Experiment in Rural Île-de-France

Interviews

Frédéric MAZZELLA, BlaBlaCar
Guy STANDING, SOAS University of London

www.idate.org

IDATE
DIGIWORLD

DIGIWORLD Economic Journal

COMMUNICATIONS & STRATEGIES

No. 108, 4th quarter 2017

DIGIWORLD
Economic Journal
COMMUNICATIONS
& STRATEGIES

No. 108, 4th quarter 2017

Dossier

The Sharing Economy: Myths and Realities

Edited by
Anders HENTEN, Denis LESCOP,
Jean Paul SIMON & Bruno SORIA

Papers

Interviews

Extra paper

Features

Regulation and Competition

Network Sharing and 5G in Europe:
The Potential Benefits of Using SDN or NFV

J. Scott MARCUS
Bruegel, Brussels, Belgium

Gabor MOLNAR
University of Colorado, Boulder, USA

Abstract: SDN and NFV provide new ways of achieving flexibility in network implementation. We explore the application of SDN/NFV technology to several promising use cases: (1) virtual unbundling in a VDSL vectoring environment; (2) as a complement to 5G's intended ability to simultaneously support multiple use cases; and (3) network sharing between mission-critical services (Public Protection and Disaster Relief (PPDR) or rail operations) and commercial mobile operations. We find that the use of SDN/NFV may be especially advantageous where multiple use cases must be simultaneously supported over time, but only if complex resource management challenges can be resolved.

Key words: network sharing, SDN, NFV, resource management, 5G, PPDR, VDSL, operational rail communications.

The sharing of fixed and especially of mobile networks is needed to address a range of current or emerging European policy requirements. Fifth-generation (5G) networks are expected to handle a range of different use cases, many of which have needs that differ greatly from one another (e.g., not only mobile broadband but also automotive and Internet of Things). The needs of these use cases can vary dynamically not only over geography but also over time (Arthur D. Little, 2017).

Software Defined Networks (SDN) and Network Function Virtualisation (NFV) are two distinct but possibly mutually complementary technologies that might be employed, either alone or together, to achieve greater flexibility as to how communication networks are used.

DigiWorld Economic Journal, No. 108, 4th Q. 2017, p. 113. www.idate.org

Research question addressed

It has become commonplace to assume that SDN and NFV, either alone or together, provide the solution to configuration flexibility going forward; however, rather little has been done to date to explore concretely how this might be done. With that in mind, our work is motivated by the need to find preliminary answers to three key questions:

- To what extent might the use of SDN and/or NFV technology be used to address these varying requirements within a common network?
- What practical, technological, economic, and regulatory policy implications might flow from the use of SDN and/or NFV in this way, and what are the interactions among these different dimensions?

Our approach to the problem

Network sharing plays, or could play, many potential roles under the European Regulatory Framework for Electronic Communications (RFEC, 2002)[1] and under its proposed successor, the European Code (EECC, 2016)[2]. In order to provide some concrete context for an exploration of the practicality of using SDN and/or NFV to address regulatory and policy needs, we consider several concrete examples or use cases where SDN/NFV technology appears to have promise: (1) virtual unbundling in a VDSL/vectoring environment; (2) as a complement to 5G's intended ability to simultaneously support multiple use cases; and (3) network sharing between mission-critical services (Public Protection and Disaster Relief (PPDR) or rail operations) and commercial mobile operations.

Given the somewhat *avant-garde* nature of what we are covering, this paper takes the form of a series of thought exercises. For each use case, the paper explores the degree to which SDN and/or NFV could address the challenges noted, and whether doing so would offer advantages (or present any disadvantages) in comparison with more traditional approaches.

---

[1] The Regulatory Framework for Electronic Communications (RFEC) is comprised of the Framework Directive (2002/21/EC), the Authorisation Directive (2002/20/EC), the Access Directive (2002/19/EC), the Universal Service Directive (2002/22/EC), and the e-Privacy Directive (2002/58/EC).

[2] See "Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code" (COM/2016/0590 final).

Structure of this paper

We provide overall background on SDN, NFV, and their relationship to 5G in Section 2. Our task in each of the three subsequent chapters is, for each of the use cases (representing policy or regulatory domains), (1) to identify relevant policy requirements, (2) to delineate relevant technical, operational, and business arrangements needed in order to fulfil the requirements using SDN and/or NFV, and (3) to reflect on specific challenges and how they might be addressed. Our conclusions appear in Section 6.

■ Relevant technical capabilities of SDN, NFV, and their relationship to 5G networking

According to analysts, the worldwide market for SDN and NFV is growing steadily each year. The global market size will exceed $10 billion by 2020[3]. We now review why these technologies are achieving such rapid market acceptance, and how the benefits of SDN and NFV apply to 5G networks.

SDN and NFV

SDN separates the network's control from the forwarding function, centralises network control, and makes the behaviour of the network devices programmable (Figure 1). Separating the network's control plane (i.e., the control logic) from the data plane (i.e., from the networking devices) has three key advantages. First, network control becomes logically centralised[4]. The SDN controller can present network services to the Application Layer and can use the packet switching and forwarding services of the Infrastructure Layer. Second, network control becomes software-based and versatile. Network administrators can rapidly respond to changing needs, can allocate network resources on demand, and can change policies easily.

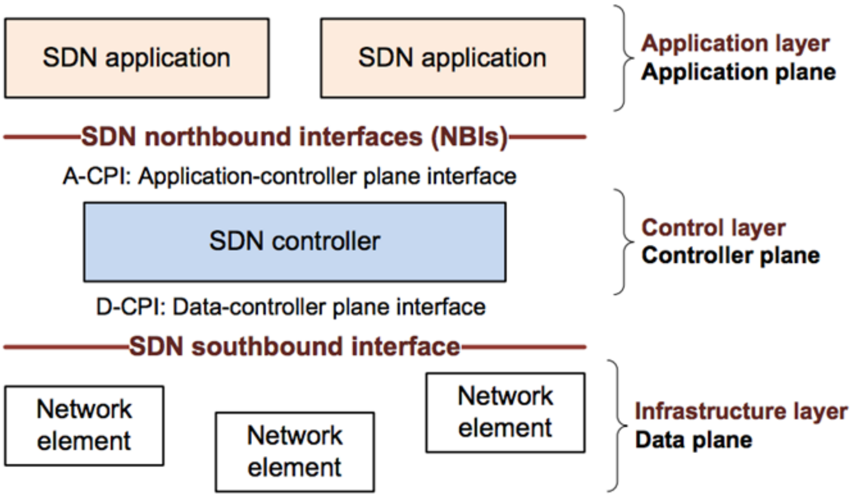
---

[3] Market size estimates by analysts vary, but the estimates confirm a rapid growth in SDN and NFV adoption. See, e.g., http://www.businesswire.com/news/home/20160203005954/en/SDN-Market-Experience-Strong-Growth-Years-IDC, viewed 27 November 2017, or https://www.sdxcentral.com/articles/news/nfv-market-worth-over-15b-by-2020-according-to-ihs-markit-report/2016/07/, viewed 1 July 2017.

[4] This centralisation is logical and is not necessary physical (KOPONEN *et al.*, 2010).

Third, network design and operation can be simpler and less expensive, because the service delivery platform does not have to include proprietary devices and protocols. The centralised view makes network operations and management very flexible and the layered architecture with well documented APIs between the layers provides independence from vendors.

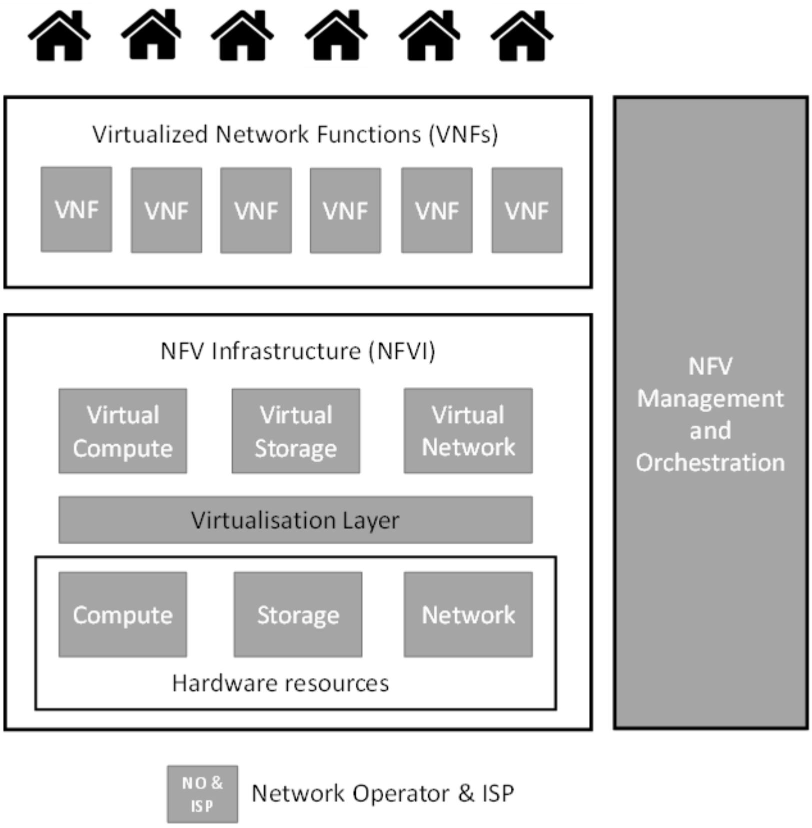
Figure 1 - High-level SDN architecture



Source: Open Networking Foundation (2014)

NFV uses virtualisation technology to consolidate heterogeneous network devices onto industry standard servers, switches, and storage. It enables network administrators to implement network functions in software, and operate the software on commodity hardware (Figure 2). Separating the network functions from dedicated hardware devices has three major benefits. First, network deployment and operation becomes flexible. Network operators can quickly make changes to the network to address changing demands and deploy network services faster. Second, deployment and operation are less costly. Network administrators can use high-volume servers instead of purchasing purpose-built hardware. Third, virtualisation allows service providers to go outside of their geographic markets and deliver the service anywhere in the world. Virtualisation also allows software to be moved to various locations inside and outside of a service provider's network, without the need for installation of hardware.

Figure 2 - High level NFV architecture.



Source: ETSI (2013)

The relationship of SDN and NFV to 5G networking

The motivations behind moving to 5G networks are many. First, existing 4G LTE and 4G LTE-A capacity cannot grow fast enough to keep up with the exploding demand driven by the growth in the number of wireless devices and data[5]. Second, cellular service providers have relatively complex management and back-office systems today, which are expensive to operate. Third, 4G service provisioning processes are manually intensive

---

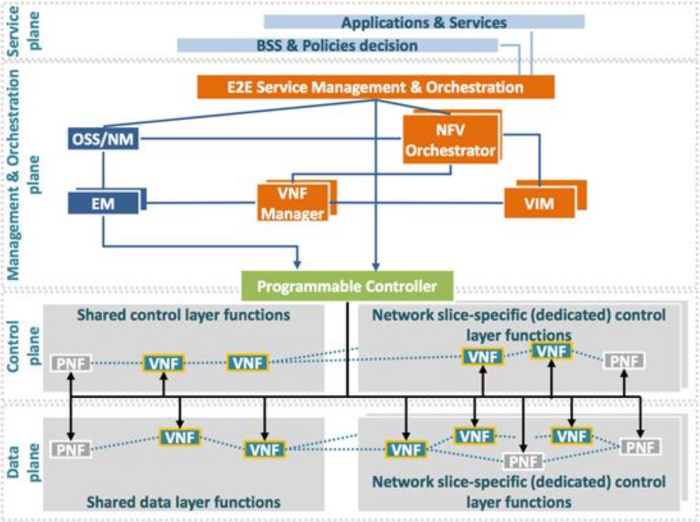
[5] Centralised data plane functionalises in the 4G network architectures causes serious scalability issues.

and rather complex making the introduction of new network functionalities and services rather slow and cumbersome.

A software-defined 5G network allows the control of the service nodes and resources depending on services required, time, and locations. It also provides support for the dynamic adjustment of bandwidth in the mobile backhaul and backbone, based on the real-time traffic load. The SDN controller in 5G networks would orchestrate the communication between the mobile devices and the applications and services in the cloud. With centralised and software-based network control, network administrators could allocate cloud-based resources on demand and could change policies quickly.

Figure 3 presents an architectural diagram showing both mobile network functionality and management and orchestration functionality. The architecture includes an E2E Service Management & Orchestration module and a software programmable controller to flexibly configure and control Virtualized Network Functions (VNFs) and Physical Network Functions (PNFs).

Figure 3 - High-level 5G architecture with software based network control



Source: 5G PPP Architecture Working Group (2016)

One of the main challenges in the 5G architecture design using SDN and NFV is determining how to transform physical access networks into multiple virtual and isolated networks while maintaining and managing seamless connectivity[6]. Mobile networks must deal with user mobility, management of the radio resources, and resource scarcity in the wireless environment. Some of the mobile applications may not only require reliable connectivity to the cloud, but they may also demand high capacity and/or low-latency. Addressing various requirements simultaneously risks increasing device complexity, degrading network performance, or impairing connectivity (BRADAI *et al.*, 2015).

There are additional questions, which will necessarily remain open until we see multi-vendor implementations and large-scale field deployments. First, can the standardisation be finalised in the time frame that we expect today?[7] Second, can the performance of SDN/NFV equipment be comparable to that of the more traditional network elements in use today, and can SDN/NFV technologies be applied to large-scale, heterogeneous 5G networks? Third, how can automatic NFV management and organisation (MANO) be implemented in practice in 5G networks – can the traditional OSS and EMS functions be executed automatically by MANO?

5G standards and resource management

5G networks are expected to support a vast number of new devices and a broadening range of new applications, including device-to-device communications, agile networks, and highly reliable low-latency industrial applications. To make things even more complex, some of the needs of the new devices and different applications may vary dynamically over time, thus requiring a more scalable and more flexible architecture.

5G critically depends on standards to ensure interoperability, security, privacy and data protection. Multiple standards organisations (ITU, 3GPP, IEEE, ETSI, ONF), industry alliances (NGMN, SCF), and regional 5G initiatives (5G-PPP, IMT-2020 (5G) Promotion Group, 5GMF), are working to define key building blocks for 5G and to feed the standardisation activities (BLANKO *et al.*, 2017). Requirements for dynamic mobility management

---

[6] Architectural discussions are outside the scope of this paper but for a comprehensive overview see 5G PPP ARCHITECTURE WORKING GROUP (2017).

[7] The final 5G specifications developed by 3GPP should be submitted to the ITU's International Mobile Telecommunication (IMT) system process for standardisation in the 2020 timeframe. See: http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx, viewed 27 November 2017.

across heterogeneous networks or resource allocation to support network slicing are all hot topics for the Standards Developing Organisations (SDOs). The consensus is that 5G will leverage SDN and NFV for flexible network management to deal with the requirements from the various use cases, but much additional work is needed to define in detail how this might be done.

The importance of efficient coordination among network elements and optimal resource utilisation in heterogeneous mobile networks is well recognized by the 5G stakeholders. There are several ongoing research projects addressing agile resource management[8]. These projects are not yet completed, and it is still unclear how agile resource management can be and will be implemented to support the 5G use cases. Indeed, the extent to which the SDN and/or NFV technology might be used to address the varying requirements of different use cases within a common network, and the practical, technological, economic, and regulatory policy implications that might flow from the use of SDN and/or NFV in 5G networks are interesting questions that constitute the primary focus of the remainder of this paper.

■ Use Case 1: Sharing copper lines within a bundle using VDSL vectoring

With current technology, the sharing of hard-to-replicate lines in order to maintain competition is difficult or impossible where VDSL/vectoring is used. For this reason, policymakers in Europe have shown an interest in virtual unbundling (VULA). Again, could SDN/NFV enable a more flexible means of allocating a single line to different network operators, on either a dedicated or on a shared basis?

The policy requirement to be fulfilled

Much of the literature tends to focus on broadband access technologies where fibre reaches all the way to the home (FTTP/FTTH); however,

---

[8] For example:
METIS-IT (https://metis-ii.5g-ppp.eu/wp-content/uploads/publications/2015/2015-10-CNCN-Agile-Resource-Management-for-5G-A-METIS-II-Perspective.pdf, viewed 1 July 1, 2017), and 5G Xhaul
(https://5g-ppp.eu/wp-content/uploads/2015/07/20150702-EuCNC-5G-XHaul-5G-PPP_V1.0.pdf).

technologies based partly on existing copper not only are the most often used last-mile connection in Europe[9], but have experienced stunningly rapid growth in some European markets (for example, in Italy)[10] in recent years. Where copper sub-loop lengths are suitable, these technologies can be much more cost-effective than purely fibre-based solutions (PLÜCKEBAUM *et al.*, 2014). Moreover, the access technologies used to exploit the existing copper infrastructure are rapidly improving. Vectored VDSL2[11] and G.fast[12] enable Internet Service Providers (ISPs) to deliver hundreds of Mbit/s to their subscribers' premises by re-using the legacy copper wires between the access node and the customer premise equipment (CPE).

Vectoring is a form of noise cancellation among different copper sub-loop pairs in the same copper bundle. Under currently available technology, there is no way to implement this noise cancellation if individual copper pairs are controlled by different DSLAMs. Shared control of the all copper pairs in the bundle is thus essential. Shared control within a single DSLAM is not consistent with regulatory obligations to provide wholesale access by means of unbundled local loops (where each network operator would provide its own DSLAM). This requirement has driven an interest in many of the Member States in a form of wholesale access known as virtual loop unbundling (VULA).

Beyond this, virtualising the control and management functions at the edge of the network might possibly enable network operators to reduce their operational expenses, to improve the control and management of their broadband access services, to achieve more flexible and faster service creation, and to improve in service quality.

---

[9] http://point-topic.com/free-analysis/fixed-broadband-subscribers-q4-2016/, viewed 15 June 2017.

[10] European Commission (2017), "Europe's Digital Progress Report - 2017: Telecoms chapter: Italy". "According to the data of the Digital Economy and Society Index 2017, NGA coverage rose significantly from 41% of households in 2015 to 72% in 2016."

[11] Vectored VDSL2 (ITU-T Specification G.993.2 with vectoring added in G.993.5) is a DSL protocol standard that allows to transmit bi-directional data over a single copper pair at 100Mbps or even higher. Vectoring is using physical layer signal processing to enable cancellation of crosstalk between the lines that terminate on a single DSLAM (ITU-T, 2015).

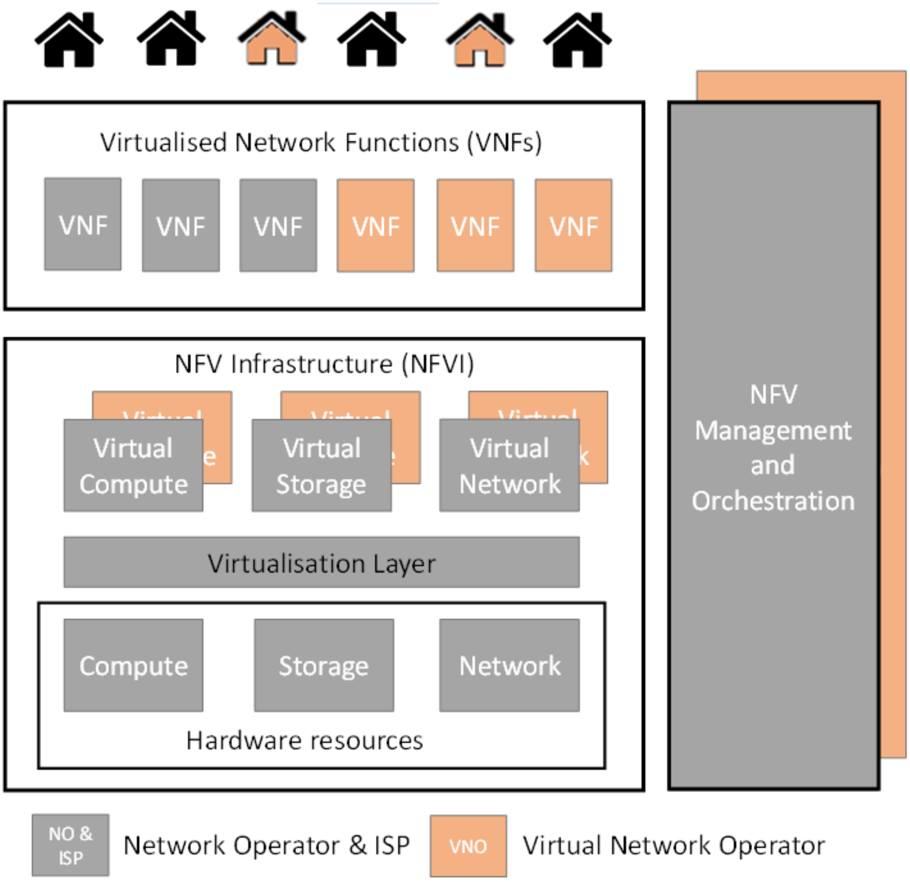
[12] G.fast (ITU-T Specification G9700 and G.9701) is a DSL protocol standard that allows to transmit bi-directional data over a single copper pair at bit rates between 150 Mbit/s and 1 Gbit/s (PUTTEN, 2014).

Technical, operational and ownership models

There are three operational models for implementing SDN/NFV in hybrid fibre-copper (HFC) networks. In the first and simplest model, there is only one player who acts both as the Network Operator and the Internet Service Provider. This operator can use SDN/NFV to centrally control and manage the subscriber lines connected to the access hardware. Control functions include the optimisation of the physical layer configuration of the broadband connection while management functions include network diagnostics and analytics. Centralising the control and management functions enables the use of more sophisticated software packages running in powerful but standard servers instead of relying on more limited software features available in vendor-specific hardware products. The model allows for homogeneous, vendor-agnostic management of the access hardware, and it does not require hardware changes because it is using the existing management interfaces. This operational corresponds to Figure 2 which appeared earlier in this paper. In the second model, one network operator runs the physical access network infrastructure but the network is shared among multiple network operators, each acting as a Virtual Network Operator (VNO). In this model, the physical network is partitioned by software into virtual networks corresponding to each network operator.

The physical access hardware is mapped into a virtual hardware and each network operator is controlling and managing its own virtual network. This model greatly improves the network operator's information about and control over the access network as they have indirect, software-based control over the network operator's hardware. This model lets the network operators design their own service offerings, and make real-time changes on the access network. The access hardware interfaces with multi-operator software that implements a virtualisation and management layer. The network operator and all the ISPs have access to functions for diagnostics, analytics, and optimisation, which are configured to meet their specific but particular objectives.

Figure 4 - An operational model where one network operator runs the physical access network infrastructure, but the network is shared among multiple network operators



Source: J. Scott Marcus and Gabor Molnar (2017)

The third model is similar to the previous one whereby we have one Network Operator and multiple ISPs, each acting as a Virtual Network Operator (VNO). In this scenario, however, the SDN and NFV extend beyond the access segment to customer premises and to the end-user network. Each network operator has access to data regarding consumer experience and broadband performance from platforms monitoring end-user devices, services, and networks. This additional data is used to better monitor access services and tune performances to meet end-user needs, which expands the ISPs' abilities to improve customer experience and offer new types of services. Examples of such services include home-network security monitoring service by the network operator, or Wi-Fi network traffic management and speed-boost capabilities by using multiple fixed or wireless links.

Any of the three models appears to be capable of achieving the crucial objective here: a partitioning of network capabilities such that a single DSLAM can manage multiple lines within a single bundle of copper sub-loops. The first model is the simplest, and appears to be sufficient to address VDSL vectoring requirements. The second or third models appear to be workable, and might be preferred for one reason or another.

Challenges and possible solutions

In each of these three models, resource management poses key challenges - not so much in terms of technology as of management and administration. These challenges relate to economic and business considerations, and potentially also raise regulatory concerns (or fail to alleviate the concerns that are already in evidence).

The firms that share the copper pairs compete with one another for the same end-user customers. If one of the firms manages the shared DSLAM for its own advantage, it might easily have both incentive and ability to disadvantage the others. This problem could perhaps be addressed at a contractual or regulatory level – if the DSLAM is managed by a wholesale-only network operator that offers no retail services (and thus does not compete with its wholesale customers), and if it has no affiliations with its wholesale customers, it should have no incentive to prefer one customer over another.

Resource management is nonetheless complex. There might well be bottlenecks involving shared resources, such as the processing power of the DSLAM or the backhaul capabilities to the long haul network. For cost reasons, these capabilities will tend to be sized to assume some statistical multiplexing among the end-user traffic streams; this implies, however, that overload is possible from time to time if all end-users happen by chance to be fully active at the same time. This problem could perhaps be addressed by a combination of (1) contracts that specify Service Level commitments in statistical terms; and (2) sophisticated dispatching algorithms to manage capacity within the devices (DSLAMs in this case).

These dispatching algorithms will probably need to be far more sophisticated than simple First-Come-First-Served (FCFS) or prioritisation algorithms; however, the problem is not hopeless. There has been considerable work over the years in dispatching algorithms for large time-shared computers that seek to achieve some notion of a "fair share" of processor resources. This work is informed not only by the mathematics of queueing theory, but also by its application to process scheduling (CONWAY *et al*., 1967).

There may also be a need to pay special attention to consumer privacy (with implications for security). Customers of one network operator should not be able to inspect the data of users of other network operators (or, for the matter, the data of other end-users that are customers of their own network operator).

■ Use Case 2: Complementing the ability of 5G to simultaneously support multiple use cases with very different requirements

The emerging 5G technology seeks to address a range of different use cases. Akin to the previous examples, these may have widely divergent sets of requirements. Mobile broadband is mostly concentrated in cities where high capacity is needed; coverage of consumers as they travel is partly a matter of covering roads and rail routes where longer distances are involved; factory automation is much more concentrated and limited in terms of distance (Arthur D. Little, 2017).

Operational rail communications (currently the province of GSM-R) require only low bandwidth, but low and predictable response times and full coverage of rail routes (MARCUS & PUJOL, 2015). The balance between speed, capacity, and distance is complex, and interacts with spectrum needs (where higher frequencies permit greater capacity, but only over shorter distances). Moreover, requirements can be time-varying. Could SDN and/or NFV help address this, especially the time-varying elements?

Technical and operational models

Technology is evolving in ways that might make it possible to circumvent some of the challenges that 5G faces. As we have seen, 5G seeks to support an exceedingly wide range of use cases, some with the demand for high bandwidth, some with the demand for low delay, some with the demand to support huge numbers of human or computerised users with heterogeneous needs. This implies that it is inevitable to differentiate network services not only in the geographic and frequency domains but also in the broader time domain as not every capability will be needed at every location at the same time. Moreover, the ability of deployed 5G networks to support various use cases may itself evolve over time.

Historically, many aspects of mobile networks have been relatively inflexible. The locations of base stations and of fixed back-haul to the base stations fall in this category. (Fixed networks are even more bound by fixed infrastructure.) The ability to upgrade or specialise the base stations, however, is poised to make a leap in the coming years.

The partitioning of the 5G network into network slices by means of SDN/NFV potentially offers the possibility of custom tailored solutions to meet the needs of specific use cases (LEVINE, 2015). A recent white paper by Ericsson expressed this vision nicely:

> "Traditional, one-size-fits-all network architectures with purpose-built systems for support and IT worked well for single-service subscriber networks with predictable traffic and growth. However, the resulting vertical architecture has made it difficult to scale telecom networks, adapt to changing subscriber demands and meet the requirements of emerging use cases. Cloud technologies together with software-defined networking (SDN) and Network Functions Virtualisation (NFV) provide the tools that enable architects to build systems with a greater degree of abstraction – which enhances network flexibility. Cloud, SDN and NFV technologies allow vertical systems to be broken apart into building blocks, resulting in a horizontal network architecture that can be chained together – both programmatically and virtually – to suit the services being offered and scaled" (Ericsson, 2015).

Challenges and possible solutions

This applicability is perhaps obvious, but little work has been done to date to explore the practical, technological, and regulatory policy implications, nor the interactions among these different dimensions. The potential benefits of a common network infrastructure to support these different use cases are manifest. First, the core of every mobile network is a (long-haul) fixed network. A common long-haul core, with common back-haul to all base stations, offers obvious cost-effectiveness advantages. Common base stations to support a range of applications likewise offer distinct advantages, particularly when one bears in mind that the applications associated with the various use cases are unlikely to all demand peak capacity at the same time (thus offering scope for statistical multiplexing).

At one level, addressing multiple use cases in a single network is not very different from the network design challenges that every network operator routinely faces. The offered load of the network (i.e., the load that would be present if there were no capacity constraints whatsoever) is the sum of the loads offered by each of the use cases that collectively comprise the load (i.e., the set union of all loads). Coverage must be present wherever any of the use cases implies a need for coverage. Capacity must be sufficient at each location to simultaneously satisfy capacity requirements each of the use cases, taking into account (e.g. by means of the application of the mathematics of statistics and queueing theory) the requirements of each of the applications in terms of bandwidth and of expected network delay.

As in the previous examples, however, the devil is in the detail. Some network applications are far more delay-sensitive than others. A simple prioritisation of packets to be transmitted over the air (or over the back-haul links) is easy enough, but providing the bandwidth and the quality of service (QoS) that the application or use case needs is considerably more complex, particularly as overall load varies over time.

Depending on the nature of the use case concerned, the priority management that is required in many of these cases may or may not run afoul of network neutrality regulations that have been implemented in the European Union /EU) / European Economic Area (EEA) through Regulation 2015/2120[13], as clarified by the BEREC (2016) Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. Briefly stated, traffic prioritisation on the part of the network is in principle permitted where the application requires it; how this relates in practical terms to traffic management practices, however, is far from clear. Notably, Recital 9 of the Regulation states: "Reasonable traffic management measures applied by providers of internet access services should be transparent, non-discriminatory and proportionate, and should not be based on commercial considerations." How a requirement for payment might relate to payment for

---

[13] European Union Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.

traffic management measures that are transparent, non-discriminatory and proportionate is left as an exercise for the reader.

Network operators are also "free to offer services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality" (sometimes referred to as specialised services); however, the specialised services "shall not be usable or offered as a replacement for internet access services, and shall not be to the detriment of the availability or general quality of internet access services for end-users".[14]

It is clear that a strict partitioning of the network would be required so as to ensure that users associated with one use case had no visibility into data of other users; this, however, should be straightforward under any reasonable implementation of SDN and/or NFV.

■ Use Case 3: Mission-critical emergency services and operational rail communications

In recent years, European institutions have on several occasions investigated how mobile networks could be used to satisfy the public needs for Public Protection and Disaster Relief (PPDR), energy, and/or operational rail communications; currently met by the aging GSM-R technology (FORGE *et al.*, 2014; MARCUS & PUJOL, 2015). In the UK and in the US, efforts are ongoing to operate PPDR from a network shared with commercial services. Doing so raises complicated technical, operational, and policy questions. First and foremost is the issue of prioritisation – at times of stress (for instance, during a natural or man-made disaster), emergency services presumably need to have precedence over normal citizens. At these same times of stress, networks tend to be massively over-crowded with traffic from citizens who also have legitimate interests in letting friends and relatives know whether they are or not impacted.

These prioritisation issues are challenging at a policy level, and are moreover not easily addressed with current technologies. At a technical level, SDN/NFV implementations might change the game. The dynamism of

---

[14] Regulation 2015/2120 Art. 3(5).

SDN/NFV might be particularly helpful inasmuch as the needs are not static. Where there is a sporting or music event, or an incident such as a train wreck, needs could spike. Again, could SDN/NFV contribute to providing the required flexibility?

The policy requirements to be fulfilled

The differences between the requirements of public safety (PPDR) communication and those of commercial voice or data communication services are many. First, public safety agencies require high availability, reliability, and resiliency for their mission critical applications, even in harsh environments. Second, the capacity demands of emergency services are less predictable than those of traditional voice and data services, both geographically and temporally. Third, public safety agencies often use services, such as group calling or device-to-device messaging, which are not typically used in traditional communication networks. Finally, communications channels for public safety networks need priority management and guarantees for uncompromised security. Traditional public safety network technologies, such as TETRA or P25, were specifically designed to meet these requirements. Public safety network technologies such as TETRA do not, however, support the high bandwidth applications that are demanded by public safety organisations today, such as real-time video from the field to commanders at headquarters (MARCUS *et al*., 2010; MARCUS, 2013).

Mobile networks today have sufficient capacity to support high bandwidth applications. They provide widespread coverage for many predictable, day-to-day data communication requirements, and coverage could perhaps be extended (for payment) in order to cover portions of the national territory that are not adequately covered today, as is being done in the UK. Public safety network architects and other stakeholders are now evaluating whether it might be possible to take advantage of the capacity that commercial wireless broadband networks provide while also meeting the specific requirements of emergency communication systems.

Commercial networks are unlikely to satisfy every possible need. Notably, there are limits to the degree to which capacity can be expanded rapidly on an *ad hoc* basis within a small local area. *Ad hoc* expansion might be needed to address either a planned activity such as a sporting event or concert, or an unexpected incident such as a train derailment or a terrorist incident. Once again, citizen requirements might spike at the same time as public safety requirements. For both planned and unplanned cases, MARCUS *et al.,* (2010) have previously suggested rolling a mobile communications vehicle, since full coverage for every possible catastrophe would be prohibitively expensive.

As with the (primarily wired) scenarios described in Chapter 3 and the 5G mobile use case scenarios described in Chapter 4, the virtualisation of commercial wireless networks by means of SDN and/or NFV might well make it easier to design and build networks that can simultaneously support commercial needs and those of public safety. A Mobile Network Operator (MNO) could in principle construct and operate the physical access network infrastructure, could partition the physical network into virtual networks, and could offer one or more virtual networks to public safety organisations. The public safety organisations would then act as virtual network operators, would control and manage their respective virtual networks, and would have the necessary control over any complimentary add-on technologies needed to enable the features that they need.

SDN and NFV could contribute to meeting the special requirements of mission critical emergency communication networks.

- First, the logical centralisation of control functions in the context of a physically distributed system can contribute to meeting the high availability, reliability, resiliency and robustness that mission critical networks require. With the virtualisation of network functions, it is possible to build logically centralised control planes that keep good concentration properties without impairing the robustness of the entire system. The virtualisation can also contribute to migration of network functions from one device to another in case of portions of the network or supporting infrastructure are disabled by the same disaster that creates the PPDR requirement.

- Second, the usage of virtual networks could facilitate the rapid *ad hoc* reconfiguration and reallocation of available network capacity (up to the level of deployed capacity) in order to meet the episodic needs of PPDR emergency without physical intervention on the device.

- Third, special services such as group calling or device-to-device messaging tend to be easier to provision and configure with software-based networks than with traditional networks.

- Finally, the decomposition of the control plane from the data plane could potentially enable or facilitate the application of fine-grained and sophisticated rules priority management to traffic flows[15].

Similar considerations apply to operational rail communications (i.e. communications to ensure that rail functions safely and reliably, as distinct from passenger entertainment services). Rail services are similar to PPDR to the extent that requirements for reliability, resiliency, robustness, and security are extreme. Even at times of natural or man-made disaster, rail operations should be maintained to the extent feasible.

Operational rail communications has many needs that differ substantially not only from those of commercial mobile networks, but also from those of PPDR. Bandwidth requirements for operational rail communications are quite low, and are not expected to grow[16]. Coverage is often required in rural areas with few residents, where commercial networks might not be inclined to deploy. Doppler effects associated with high speed rail require special attention. Perhaps most notably, the latency requirements of the ERTMS/ETCS data systems that enhance the safety of high speed rail are extreme in comparison with those of normal commercial mobile communications – if connectivity is lost or if a response is delayed, the train stops.

Voice communications needs for operational rail are broadly similar to those of PPDR, and include capabilities such as group call and push-to-talk (PTT). Unlike PPDR, a special capability exists to facilitate the rapid establishment of a group call among a group of nearby trains. These capabilities, which are provided by rail-specific GSM-R capabilities today, would presumably need to be replaced by application level capabilities. (Similar capabilities are being designed by 3GPP for LTE, but GACH *et al.*, (2017) consider this as a limited interim solution.)

For rail communications, as for PPDR, sharing of capacity with commercial networks could offer price/performance advantages in comparison with the dedicated networks that are used almost universally today. Coverage of commercial networks would likely need to be extended,

---

[15] OpenFlow network decisions are decided on a flow basis, for arbitrary flow definition, and implemented in the form of rules with priority levels. Flows can be treated differently based on policies implemented by the controller and as the controller has a full view of the network, it ensures the strict respect of the policies.

[16] They are higher, however, in stations and in shunting yards than on long rural stretches.

which could in principle be done through public procurement processes leading to contracts between the Infrastructure Manager (or IM, typically a government-owned entity) and one or more MNOs. Security and reliability could likewise in principle be managed through contracts awarded through a procurement process.

An intriguing option relates to the possible integration of passenger rail communications with operational rail communications, given that they would require similar coverage that would not necessarily be provided by commercial MNOs in the absence of special arrangements made by the IMs (or alternatively by the Rail Undertakings (RUs) that operate the trains). Once again, resource management plays a crucial role. Passengers watching dancing cats on their mobile phones cannot be allowed to crowd out communications necessary to train safety.

Technical, operational and ownership models

Both for PPDR and for operational rail communications, the most likely operational models of interest assume that a Member State government (or a PPDR agency or an IM) select one or more MNOs through a public procurement process, and then govern the relationship with the MNO by means of contract. If passenger rail were to be included together with operational rail, the most obvious model would be for the Member State government or IM to procure and manage the communication service and to make passenger rail communication capabilities available to RUs (the entities that operate the trains) through contract.

Challenges and possible solutions

Once again, resource management issues are hugely challenging. Concerns with force majeure incidents impact all of the scenarios that we discuss in this paper, but they are of special concern for mission-critical services. They represent a key reason why the PPDR forces might be deployed in force in the first place.

As in the previous use cases, a simple all-or-nothing prioritisation is insufficient. The basic principle that would need to be followed in practice is something like:

- Mission-critical PPDR or rail operational needs get first preference for whatever network capacity is available (and bearing in mind that the network may have suffered damage), civilian customer demand notwithstanding.
- Civilian customer demand should be satisfied as fairly as possible out of the remaining capacity. Call admission control and similar techniques should be employed to avoid squandering the network's remaining capacity.

PPDR and rail operational networks are used for some administrative functions that are not necessarily mission-critical. In a shared network, these do not necessarily require higher priority than those of civilian communications. This would require careful, objective analysis.

Network neutrality rules are not an impediment to the required prioritisation. For PPDR communications and for operational rail communications, network neutrality rules are inapplicable because PPDR and operational rail communications do not provide access to the Internet, and do not serve the general public. Prioritisation might also be required for rail passenger communications, but network neutrality is again inapplicable under BEREC Guidelines (BEREC, 2016) because the EU net neutrality Regulation "does not cover providers of electronic communication services or communication networks that are not publicly available … Electronic communication services or networks that are offered only to a predetermined group of end-users [e.g. rail passengers] could be considered to be not publicly available."

Insulation of the network from commercial networks would be crucial in light of security needs – the risks if malefactors could overhear police communications, for instance, are evident.

■ Conclusions

A judicious combination of SDN and NFV could potentially enable flexible solutions to a range of public policy solutions in the future, including (1) sharing of DSLAMs in a VDSL/vectoring scenario, (2) simultaneous fulfilment of multiple use cases in a 5G mobile networking scenario, or (3) sharing of a mobile network between commercial consumer use and mission-critical use by public protection and disaster relief (PPDR) or by operational rail communications. In each case, shared use has implications for the service that is to be provided.

- Management of multiple uses implies the need for careful resource management. Where the parties sharing the network are commercial competitors, or where some services are mission-critical while others are not, the sharing of resources implies not only technical but also managerial and policy complexity.
- Network sharing between competitors entails certain complexities with which regulators are familiar, such as (1) ensuring that operational control is managed in such a one as not to favour some users over others, and (2) ensuring that information sharing (for instance, in planning for future network needs), does not needlessly expose competitive information among the participating firms.
- Avoidance of being overheard is likewise a concern in any networking scenario, but it looms particularly large in some of the shared networking scenarios explored here, including in particular those where mission-critical services such as public protection and disaster relief (PPDR) shares the network with commercial services provided to consumers.

In our view, all of these challenges can be addressed in time. The operational shared network issues are already familiar to national regulatory authorities (NRAs), and are not unique to the use of SDN and/or NFV technologies. Likewise, it is clear that the requirement not to be overheard requires a clean and complete partitioning of the networks, and will necessarily be addressed early on.

It is the resource management requirements that give us pause for thought. The challenges raised, especially in the more complex scenarios, are potentially quite severe. Several research projects touch on these issues, but solutions are not yet visible. We believe moreover that the industry is many years away from implementing and offering solid, commercially available systems that offer reliable solutions to these challenges.

If intelligently addressed, these resource management challenges might ultimately be viewed not just as a threat, but also as an opportunity. Analogous resource management challenges are already visible in existing non-SDN/NFV sharing scenarios. SDN/NFV potentially enables solutions that are more flexible, more highly automated, and less expensive to implement and to operate than traditional solutions.

References

5G-PPP ARCHITECTURE WORKING GROUP (2017): View on 5G Architecture (Version 2.0). https://5g-ppp.eu/wp-content/uploads/2017/07/5G-PPP-5G-Architecture-White-Paper-2-Summer-2017_For-Public-Consultation.pdf.

Arthur D. Little (2017): *Creating a Gigabit Society – the role of 5G*, a study for Vodafone. https://www.vodafone.com/content/dam/vodafone-images/public-policy/reports/pdf/gigabit-society-5g-04042017.pdf.

BEREC (2016): *BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*, BoR (16) 127, paragraphs 8 and 12.

BRADAI, A., SINGH, K., AHMED, T. & RASHEED, T. (2015): "Cellular Software Defined Networking: A Framework". http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7120043.

CONWAY, R. W., MAXWELL, W. L. & MILLER, L. W. (1967): *Theory of Scheduling,* Addison-Wesley, Reading, MA.

Ericsson (2015): *5G systems: Enabling Industry and Society Transformation*, Ericsson White paper 284 23-3251 UEN. https://www.ericsson.com/assets/local/publications/white-papers/wp-5g-systems.pdf.

ETSI (European Telecommunications Standards Institute):

- (2012): *Network Functions Virtualisation*, Introductory White Paper. https://portal.etsi.org/nfv/nfv_white_paper.pdf.

- (2013): *Network Functions Virtualisation*; Architectural Framework, ETSI GS NFV 002 v1.1.1 (10 2013), page 10. http://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.01.01_60/gs_nfv002v010101p.pdf.

FORGE, S., HORVITZ, R. & BLACKMAN, C. (2014): *Is Commercial Cellular Suitable for Mission Critical Broadband?,* Study on use of commercial mobile networks and equipment for 'mission-critical' high-speed broadband communications in specific sectors, Report number: SMART 2013/0016. https://www.researchgate.net/publication/289540175_Is_Commercial_Cellular_Suitable_for_Mission_Critical_Broadband_Final_Report_to_the_European_Commission.

GACH, G., MARCUS, J. S., MATON, C. & PUSHPARATNAM, L. (2017, forthcoming): *Implications of Bearer Independent Communication Concept*, a study for the European Rail Agency (ERA). ERA 2016 17 RS.

ITU-T (2015): "G.993.5". https://www.itu.int/rec/T-REC-G.993.5/en.

KOPONEN, T., CASADO, M., GUDE, N., STRIBLING, J., POUTIEVSKI, L., ZHU, M., RAMANATHAN, R., IWATA, Y., INOUE, H., HAMA, T. & SHENKER, S. (2010): "Onix: A Distributed Control Platform for Large-scale Production Networks". https://www.usenix.org/legacy/event/osdi10/tech/full_papers/Koponen.pdf.

EUROPAEAN COMMISSION:

- (2016): "Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code" (COM/2016/0590 final).
- (2017): Europe's Digital Progress Report - 2017: Telecoms chapter: Italy. http://ec.europa.eu/newsroom/document.cfm?doc_id=44448.

EUROPEAN PARLIAMENT AND COUNCIL:

- (2002): *Framework Directive*, Directive 2002/21/EC. Amended in 2009.
- (2002): *Authorisation Directive*, Directive 2002/20/EC. Amended in 2009.
- (2002): *Access Directive*, Directive 2002/19/EC. Amended in 2009.
- (2002): *Universal Service Directive*, Directive 2002/22/EC. Amended in 2009.
- (2002): *Directive on privacy and electronic communications*, Directive 2002/58/EC. Amended in 2009.

LEVINE, H. (2015): "The 2020 WAN takes shape – SDN, virtualization, and hybrid WANs". http://www.networkworld.com/article/2971214/wan-optimization/the-2020-wan-takes-whape-sdn-virtualization-and-hybrid-wans.html.

MARCUS, J. S. & PUJOL, F. (2015): *Evolution of GSM-R*, a study on behalf of the European Railway Agency. http://www.era.europa.eu/Document-Register/Pages/Study-for-the-evolution-of-GSM-R-%28by-IDATE-WIK%29.aspx.

MARCUS, J. S., BURNS, J., JERVIS, V., WÄHLEN, R., CARTER, R. K., PHILBECK, I. & VARY, P. (2010): "PPDR Spectrum Harmonisation in Germany, Europe and Globally", December. http://www.cept.org/Documents/fm-49/1552/FM49_11_Info2_WIK_Report_PPDR_Spectrum_Harmonisation

MARCUS, J. S. (2013): *The need for PPDR Broadband Spectrum*, study on behalf of TCCA. http://www.tandcca.com/Library/Documents/Broadband/WIK%20report%20on%20PPDR%20Spectrum.pdf.

Open Networking Foundation (2014): *SDN architecture, ONF TR-502*. https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf.

PLÜCKEBAUM, T., JAY, S. & NEUMANN, K-H. (2014): "Benefits and regulatory challenges of VDSL Vectoring (and VULA)", RSCAS 2014/69. http://hdl.handle.net/1814/31712.

PUTTEN, F. van der (2014): "Overview of G.fast". http://uppersideconferences.net/g-fast-summit2014/pres-gfast2014/day_1/day_1_2_Frank_van_der_putten.pdf.