European Commission

FRAMEWORK CONTRACT SMART 2019/0024 LOT 2 - EXPLORING, DOCUMENTING, AND ANALYSING DIGITAL POLICY ISSUES

5G SUPPLY MARKET TRENDS

Final Report

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Arthur D Little

imec

Fraunhofer ISI

RAND EUROPE

Internal identification

Contract number: LC-01529421
VIGIE number: 2020-0705

Authors

AIT Austrian Institute of Technology
Michael Dinges (Project Manager), Markus Hofer, Karl-Heinz Leitner, David Löschenbrand, Dana Wasserbacher, Stefan Zelenbaba, Benjamin Rainer, Bernhard Dachs, Thomas Zemen

Fraunhofer ISI
Knut Blind

Imec
Pol Camps, Simon Delaere

RAND Europe
Advait Deshpande, Salil Gunashekar, Mann Virdee
Reviewed by: Michael Bernstein, Maximilian Zieser

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology
Directorate E – Future Networks
Unit E.1 – Future Connectivity Systems

Contact: CNECT-E1@ec.europa.eu

European Commission
B-1049 Brussels

FRAMEWORK CONTRACT SMART 2019/0024 LOT 2 - EXPLORING, DOCUMENTING, AND ANALYSING DIGITAL POLICY ISSUES

5G SUPPLY MARKET TRENDS

Final Report

2021 Directorate-General for Communications Networks, Content and Technology EN

LEGAL NOTICE

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the European Commission. The European Commission does not guarantee the accuracy of the data included in this study. Neither the European Commission nor any person acting on the European Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Print	ISBN 978-92-76-40348-7	doi: 10.2759/833784	KK-05-21-235-EN-C
PDF	ISBN 978-92-76-40349-4	doi: 10.2759/017326	KK-05-21-235-EN-N

Manuscript completed in July 2021

Luxembourg: Publications Office of the European Union, 2021

Executive Summary

Background and objectives

The importance of 5G infrastructure, its fast roll-out, and technological capabilities, as well as the development of the supply side of 5G infrastructure, has been highlighted by the European Commission (EC) in various initiatives and strategies including the Communications “5G Action Plan for Europe" and ”Secure 5G deployment in the EU: Implementing the EU toolbox”. However, although Europe is home of two of the three major equipment suppliers and is world leader in trial investments in 5G, overall infrastructure investments lag behind other regions and Europe’s vertical industries are only just starting to identify valuable 5G business cases and European equipment providers are facing challenges to sustain their viability, facing increased competition from Chinese, South Korean, and U.S. manufacturers.

Against this background, this study provides an in-depth analysis of plausible developments of the 5G equipment and services supply market looking out to 2030. The study identifies 4 scenarios, determined by factors such as evolving technology, standards readiness, and Radio Access Network (RAN) disaggregation initiatives. Economic, technological, environmental, and societal impacts are analysed for each scenario, covering key EC and stakeholder concerns, including market competition, costs, cybersecurity, energy efficiency, and standards needs. Based upon the results of the scenario impact analysis, the study identifies policy options to facilitate the evolution of a viable 5G supply ecosystem in Europe.

Key trends influencing the future development of 5G

The study team, drawing upon a Horizon Scanning activity and an expert survey, identified the following eight key trends influencing the future development of the 5G supply market. Each trend represents a factor with a high potential impact on the 5G supply market but also a high level of uncertainty regarding the eventual outcome.

Open and interoperable 5G network solutions: The virtualization of the RAN and the development of new RAN architecture (full virtualization of the native 5G core network, Open RAN) are blazing a path for the implementation of open and interoperable solutions in the network.[1] Several initiatives have applied an “Open RAN” model, aiming to replace closed architectures linking proprietary networking hardware and software with more open and modular interfaces.[2] Open and interoperable 5G network solutions could provide an opportunity for new players to enter the RAN market, fostering vendor diversity and increasing the development speed and competition.[3] While open and interoperable network solutions offer notable benefits, trade-offs in terms of performance, costs, energy efficiency, cybersecurity, supplier diversity, and reliability remain areas of active controversy among the 5G community and in the literature.[4]

Emergence and entry of new players: Open and interoperable network solutions are paving the way for new players in the 5G supply market. While Open RAN may set enabling conditions for new network vendors, it is not a singular feature driving emergence or entry. New entrants may emerge from established companies with strong competencies in hardware, baseband provision, or software services. In addition, new key players may also emerge from start-ups or other sectors.

Level of Public R&I investments for EU players: Current European R&I investment in 5G development is low compared with international benchmarks (APAC).[5] Increased R&I investment for European players could help the 5G innovation ecosystems thrive.

1 Pujol et al. (2020b)
2 Plantin (2021)
3 Pujol et al. (2020b); Hofer (2020)
4 See for instance Barford (2021)
5 Taga et al. (2021)

Degree of pan-European cohesion and scale in public initiatives: Government 5G investments in Europe have historically occurred on a national level, creating a challenging environment for achieving pan-Europe public initiatives with high cohesion and at scale. While some European states have launched and are progressing national 5G programmes of variable size, others lag behind.[6] Existing small-scale programmes at the national level focus on research and piloting rather than broader implementation across Europe. Recent active guidance from the European Union, including the 5G Infrastructure Public-Private Partnership (5G-PPP) and the Joint Undertaking on Smart Networks and Services towards 6G (SNS JU) proposal, is beginning to address this challenge.[7] The European 5G-PPP represents a 3.5 billion Euro investment in 5G of which 700 million is public investment.[8]

Policy support for new actors: Funding and financial support for new players entering the 5G supply market could help facilitate 5G deployment and increase the diversity of European 5G supply market actors.

Development of vertical markets and industries: Developments of 5G application possibilities in vertical markets and industries has implications for future 5G supply markets. Ongoing and profound digital transformation of vertical industries, such as health and healthcare, industry 4.0 and manufacturing, automotive and transport, AR&VR&MR and mining, could create a transformational level of demand for 5G supply. Along with the development of vertical markets and resulting novel 5G use cases, the creation of private 5G networks offers another important new revenue stream for incumbent network operators, vendors, and possible new integrators.

Security challenges in 5G networks: As part of a series of digital industrial transformations, 5G networks will become increasingly critical infrastructure for the functioning of public and private sectors. With such expected growth, security challenges are likely to grow in prominence as well[9]. These challenges include threats to the availability and integrity of networks, increased exposure to attack, and high-risk exposure of critical suppliers in the 5G ecosystem.

Universal standards and open specifications: An advancement of 3GPP specifications and releases, along with standard-essential patents (SEPs), could further promote agreements on universal standards for 5G. Universal standards could in turn open the supply market landscape to smaller hardware and solution providers or start-ups, further promoting the diversity of players in the 5G supply market.

Impact analysis of four plausible development scenarios

Based on the trends outlined above, we constructed four plausible scenarios of 5G development in Europe for the time horizon of 2030. The results of the scenario development and impact analysis highlight the current uncertainty and diverging assessment and expectations regarding Open RAN in the short- and medium- terms.[10] While scenario I and II can be considered as pathways which might become reality on the short to medium term, scenario III and IV can be considered rather as medium and long term pathways.

Scenario I: Incumbent players driving 5G

Key Storyline: Incumbent vendors and MNOs are shaping the ecosystem pulled by increasing demand for new services from verticals requiring high performance. Equipment from providers considered a security risk is used outside a core network and in non-sensitive areas only. The adoption of Open RAN for specific applications and in specific regions sets incentives for established vendors to further improve the efficiency of their proprietary solutions. Incumbent network equipment

6 Taga et al. (2021, S. 12)
7 See the SNS proposal: https://digital-strategy.ec.europa.eu/en/news/europe-puts-forward-proposal-joint-undertaking-smart-networks-and-services-towards-6g.
8 Taga et al. (2021, S. 12)
9 European Commission (2019)
10 see Barford 2021; Plantin 2021

vendors continue to operate successfully but new equipment providers emerge, further facilitating network integration. Cloud RAN and vRAN are important intermediate steps for MNOs on their investment paths. In the short run, Open RAN solutions developed mainly exist in niche areas and do not yet serve as game-changers in the 5G ecosystem.

Impact Analysis: In Scenario I, it is assumed that incumbent vendors and MNOs orchestrate the emerging 5G innovation ecosystem. The opportunity for MNOs in a context of more open interfaces is that orchestration efforts bring new equipment suppliers and lower prices. However, only the largest incumbent MNOs—those with enough R&D activities and financial capacities in place—may start to build and orchestrate an incipient ecosystem of new component suppliers. **Supply market competition** in Europe increases slowly. Incumbent vendors may maintain their market share and play a decisive role in the development of Open RAN.

The emergence of new vendors will focus on the increasingly relevant **private-sector networks**. These new networks provide significant opportunities for new vendors, as there are no path dependencies when compared with large European consumer markets. A risk for both MNOs and traditional vendors is that revenue opportunities in these emerging markets may not be realized because of MNOs' and vendors' comfortable position in the large consumer market.

In terms of **costs**, MNOs find it financially feasible (or even beneficial) to invest in vRAN and Cloud RAN as intermediate solutions. In the long run, MNOs gradually introduce Open RAN (even if proprietary) deployments. Traditional vendors anticipate these developments and adjust their prices at least to some extent. As a result, total operating costs decrease for MNOs.

Business models and system integration for the supply chain are likely to remain largely unchanged in the medium term. Only large MNOs may feel confident to explore white-box models and potentially adopt an in-house model of system integration in the future.

The overall pace of **modularisation and decrease of supplier dependency** is moderate. The emergence of **new services and applications** in this scenario may only occur gradually as incumbent MNOs and vendors with their focus on hardware may not be the most suitable actors to introduce new services. The decade-old search of MNOs for a 'killer app' that pushes demand for new generations of mobile communication is a testament to this claim. For 4G, US social media and software companies introduced key services and drove the growth of mobile data. We may therefore expect that services will emerge as a continuation of, rather than a radical departure from, existing services.

Cybersecurity risks can be largely contained as MNOs and incumbent vendors invest in risk mitigation measures, which also secures market advantages for themselves. A strong role of incumbent vendors and MNOs may also be beneficial for **energy efficiency** as system performance might be better tailored to integrated stand-alone solutions.

In terms of **standard-setting measures**, O-RAN standards set by 3GPP complement the RAN standards. While this constitutes an opportunity to increase competition and thus reduce the dependency on few remaining suppliers, the threat in this scenario is that limited involvement of stakeholders in the standardization process jeopardizes acceptance of O-RAN specifications.

The contribution of 5G in Scenario I is expected to be the same as the current contribution of 4G technology to Europe's economic growth, and that **we will not see a boost to turnover or employment** in Europe as evidenced by the previous introduction of new mobile network technologies.

Scenario II: Slow pace of 5G Roll-Out

Key storyline: MNOs and vertical industries struggle to find the right business case for 5G. Consumers demonstrate indifference towards higher broadband speeds offered by highly-priced 5G networks and are contented with service over a wide area with 4G. 5G-based industrial services emerge only slowly. A fragmented approach to the implementation of cybersecurity requirements in Europe leads to legal uncertainty regarding supplier requirements. A fragmented approach also contributes to long transition periods for any multi-vendor strategies. Simultaneously, conditions for increasing multi-vendor interoperability via standards-based interfaces are not being reached in the medium term. 5G deployment in Europe in consumer and business markets is of modest speed. MNOs slowly start providing end-to-end Open RAN networks, primarily in suburban and rural areas.

Impact analysis: In this scenario **market competition** remains the same or even decreases due to the exclusion of vendors because of geopolitical motivations and/or security concerns. Due to the low uptake of B2B use cases, the overall 5G market size does not expand in Europe and the slow 5G rollout does not provide opportunities for new vendor solutions to be scaled.

For the 5G supply market, this scenario resembles the status quo most starkly in terms of **costs**. Compared with the status quo, equipment prices may even increase if no alternatives for equipment providers manage to enter the market.

In terms of **business models for system integration**, the predominance of the traditional integrated model is unlikely to change in this scenario. Similar levels of **modularity** cause vendor lock-in and hence supplier dependency to persist. Consequently, potential adverse effects from system disaggregation are less likely.

New 5G based **services** cannot be introduced rapidly in an environment sketched by this scenario, and segmented geographical markets may further hamper the roll-out of Europe-wide services. When national policy pushes their introduction, health services may benefit appealingly in this scenario, but their introduction might also be hampered by the lack of performance and diffusion of 5G.

Cybersecurity is not such a big issue in this scenario, as this scenario gives more time to reflect on the risks in advance and mitigate them within traditional, integrated systems and clear overall responsibilities. Despite existing **energy efficiency** inefficiencies of 2G/3G/4G networks an overall slow 5G roll-out in Europe might delay any overall increase in data usage (likely in the opposite case of ubiquitous 5G network availability) leading to decreased energy intensity.

The scenario has negative implications for **standardisation** for both 3GPP and O-RAN Alliance due to a lack of feedback from the applications of 5G standards in practice back into standardisation.

The overall **economic impact for Europe** is negative. The slow 5G roll-out in this scenario may be partly compensated by the favourable conditions for European suppliers of 5G equipment. Nevertheless, the negative effects from a delayed roll-out are larger than the positive effects for European suppliers in this scenario.

Scenario III: Open RAN as a game-changer

Key storyline: In this scenario, it is envisioned that technological progress is impressive and Open 5G platforms enable standardised services on fully virtualised networks in the medium and long term. The demand for new 5G services is created by verticals that are served by MNOs but also new entrants specialised in operating networks. Established MNO, incumbent vendors, verticals, and new entrants build up the 5G innovation ecosystem and new solutions for factories or autonomous driving are on the rise. Open RAN solutions drive suburban offerings and broaden the range of services in rural areas. MNOs face competition by new European and non-European operators who enter the industry to serve specialized areas. New operator entrants, in turn, accelerates interest by verticals. Policy support for pilot projects in collaboration with verticals pushes applications, generating amplifying feedback.

Impact analysis: In this scenario decentralized, disaggregated and fully virtualized Open RAN networks serve Europe. The uncertainties of Open RAN are resolved in the medium term, leading to increased **market competition** and new suppliers in the RAN domain. Development efforts for new business opportunities for traditional vendors are high to remain competitive. Regarding new vendors, the most plausible outcome from a present perspective is that **non-EU entrants lead absorption of new demand**.

The **costs** for equipment (CAPEX) go down due to competitive pressures. The level of competition is high, and so is the scale of deployments. Operational expenses of Open RAN deployments catches up and may finally even outperform traditional ones. In the longer term, there is a threat of re-consolidation in the market, which could reverse the expected benefits realized by fully virtualized Open RAN networks.

System integration costs remain a key challenge due to increased complexity. High uncertainties regarding overall cost savings bring opportunities for traditional vendors, which could take early leadership in Open RAN and make sure that new players develop under their leadership.

The market for new **services** and applications is characterized by a high level of competition, entry of new players and strong demand by verticals.

Supplier dependency decreases and vendor lock-in in the RAN becomes a problem of the past for MNOs, while challenges at the system integration level increase, because of high modularity.

Cybersecurity risks are a key challenge. While interoperability increases, cybersecurity risks may be exacerbated as the diversity of providers seeking interoperability provides more entry points for hackers, irrespective of the vendor. Increased heterogeneity of networks makes it also more difficult to realise power gains. **Energy efficiency** and energy consumption become a challenge, as it may become more difficult to measure and control energy consumption in each part of the network and energy consumption might increase due to optimisation on flexibility and interoperability.

Interoperability and therefore **standards** will become more relevant. The O-RAN architecture and its specifications would become (defacto) standards for RAN. The O-RAN architecture will attract new suppliers, which might eventually contribute to standardisation both at 3GPP and the O-RAN Alliance. To handle the complexity, MNOs can opt for a subset of suppliers and proprietary implementations of Open RAN solutions.

For Europe, this scenario offers some possibilities (new opportunities for European suppliers, MNOs, service firms, and in particular vertical industry) but also risks (dominance by non-European firms, EU vendors may significantly lose market share).

Scenario IV: 5G for Big Tech

Key storyline: Network virtualisation and disaggregation of software and hardware change the landscape for network equipment, deployment and service provision in the long term. New business models based on Open RAN architectures and interfaces gain momentum and new major players enter the market. Complete 5G solutions encourage companies from vertical industries to enter the market. MNOs are not able to find their role as infrastructure providers for industrial players and are outflanked by Big Tech companies who also offer services to end-users. Big Tech become the "new operators" and will serve as virtual operators.

Impact analysis: In this scenario, foreign Big Tech companies increase their overall dominance in the **market** on demand and supply sides alike. As network functions and elements become increasingly virtual, Big Tech players may leverage their cloud and software capabilities to move into connectivity and supply domains with innovative solutions. Moreover, their financial strength allows them to overtake existing players and new entrants.

However, their specific entry to the markets for B2C connectivity and RAN equipment may be unrealistic. For Big Tech the core network might be more interesting than the RAN because the core network is easier centralised, and closer to their current skills and infrastructure, based on cloud computing in data centres.

The key threat for market competition by Big Tech is on the demand side. As added value will shift from connectivity itself to the cloud, the future value generation of MNOs may decline. Another realistic threat is that Big Tech players dominate the end-user services by offering more value-added OTT services, and MNOs remain stuck offering the least profitable part of the chain, i.e., becoming 'dumb pipes'. Additionally, Big Tech companies may enter the connectivity provision market and increase competition.

In terms of **costs**, the impact on RAN-related OPEX is low. Tech companies only take over a small part of a base station’s processing. However, the higher bargaining power and overall dominance of Big Tech threatens to keep the prices of their solutions high.

Concerning business models and **system integration requirements,** the key threat for European MNOs is that foreign Big Tech players become the go-to integration option. On the demand side, Big Tech business models based on their cloud and OTT services help Big Tech to increase their dominance. While a vendor lock-in for the RAN might be substantially reduced, a new reliance on large foreign players threatens to bring a new bottleneck in the supply chain (e.g., at the cloud level).

New services and applications - the main driver for 5G added value and new revenues for firms - would be dominated by non-European Big Tech. A use case that would benefit in particular in such a scenario is Connected and Automated Mobility (CAM). Another area where use cases may benefit from complementary competencies within Big Tech companies is health.

As regards **cybersecurity**, Big Tech is not necessarily more secure than medium or small tech – but the scale of people reached with any single vulnerability is likely to be greater. Concerning **energy efficiency**, Big Tech might be beneficial for energy reduction because large tech companies already manage energy in data centres.

Big Tech companies in this scenario become dominant also in **standardisation**; their influence in the O-RAN Alliance might become bigger, reducing the relevance of existing players. However, they could also start offering non-O-RAN proprietary solutions.

Thanks to the fast roll-out of 5G and the emergence of a vivid services eco-system, Scenario IV offers some opportunities for Europe. Studies on the economic impacts of 5G have shown that these are largest when 5G diffuses fast. If Industry 4.0 is a fast-growing use case, it may provide opportunities for Europe’s large manufacturing base in particular. Several industrial firms may extend their product range to 5G based services.

But there are also key risks for Europe associated with this scenario. The fast diffusion of Open RAN may allow non-EU companies to take a good part of the MNOs and suppliers market. Given the weak market position of Europe in many software and services markets, it seems uncertain whether European companies will make the best of these new opportunities. Much will depend on if non-European firms will operate these new businesses via European affiliates or directly from their home countries.

Policy recommendations

Establishing a viable 5G supply ecosystem requires a combination of system-oriented policy measures, which aim to mitigate risks of the scenarios on the one hand while seizing their long-term opportunities on the other hand. The policy measures should ultimately contribute to the following overarching goals:

- The EC and the EU Member States should develop an open and secure 5G ecosystem in the long run, including MNOs, incumbent and new European vendors, software providers including open-source communities, and European users from vertical industries.
- The EC and the EU Member States should promote European digital autonomy and technological sovereignty via the support of collaboration between new and traditional vendors, and a strong approach towards open specifications in the 5G ecosystem.

The study details specific policy recommendations important for the development of a viable 5G ecosystem:

R&D investments are needed across the whole supply chain, from basic research to experimental development to trials to, pilots and large-scale deployment. In particular, the security dimension should be considered. The study recommends supporting R&D projects related to 5G, with a focus on the collaboration between large companies and small companies located in the EU to promote the 5G ecosystem in the EU. New R&D funding initiatives focusing on 5G should in particular target SMEs and start-ups. The development of regional clusters of excellence and smart cities in the area of 5G technologies and services should be encouraged, including partnerships between industry, research organisations, Open-source communities and the private sector. The study also recommends supporting the identification and development of business models or use cases for verticals related to 5G networks and applications.

Standardisation and the resulting standards, testbeds, and certifications are crucial for the development of mobile telecommunication networks, as is shown by the massive efforts in 3GPP and the different generations of 5G standards as well as the creation of the O-RAN Alliance. To avoid fragmentation or a lack of interoperability, the required standards should be developed at the global level. Compliance with the O-RAN Alliance to the Code of Good Practice when developing standards released by the WTO and the EU Regulation No 1025/2012, closer collaboration between 3GPP and the O-RAN Alliance, and a European Certification Scheme applicable for products related to 5G are important cornerstones in this regard.

The ecosystem diversity benefits from the **entry of start-ups** and companies from other domains. In addition, technological sovereignty or digital autonomy, the EU needs to **foster entrepreneurship** in 5G related technologies, business models and services. To address the lack of venture capital in the European small business ecosystem, it is recommended to continue the Enhanced EIC programme (including the EIC Accelerator) and explicitly open it to applications from young, high-risk, R&D-intensive entrepreneurs that focus on 5G-related technologies and business models.

Public procurement can stimulate innovation and growth through public sector demand. The public procurement of networks is becoming increasingly important to strengthen the European supplier landscape. Therein, it is recommended to fully exploit the potential synergies between commercial procurement and standards related to 5G technologies by referencing 3GPP and O-RAN Alliance specifications and standards instead of proprietary specifications. The procurement processes should follow EU-wide public procurement guidelines and recommendations, particularly taking into account the needs of SMEs and start-ups. Finally, the potential synergies between commercial procurement and 5G-related Open-Source technologies need to be considered more strategically and systemically.

Also, the **regulatory framework** plays an important complementary role. All regulations should be based on the principle of technology neutrality. An effective **competition regulation** can promote both the 5G ecosystem as well as digital autonomy or technological sovereignty. Concerning **security,** it is recommended to support risk assessment schemes for vendors in the 5G supply chain based on clearly operationalized and transparent security regulations. Concerning **energy efficiency,** it is recommended that the potential improvement of energy efficiency in the context of 5G are considered in future environmental regulations and standards, e.g. via specifying energy-efficient targets for 5G technologies and networks complemented by financial incentives for energy-efficient solutions.

TABLE OF CONTENTS

Abbreviations

Abbreviation	Meaning
3GPP	3rd generation partnership project
5GC	5G core
AAU	Active antenna unit
AMF	Access management function
APAC	Asia-Pacific Countries
AR	Augmented reality
ARPU	Average revenue per user
BBU	Baseband unit
BM	Bare metal
BSS	Business support system
BTS	Base station
CAPEX	Capital expenses
C-Band	3.4–3.7 GHz
CEX	Customer experience
CNF	Core network function
COTS	Commercial off-the-shelf
CPU	Central processing unit
C-RAN	Centralized/Cloud RAN: Concentrating and consolidating the baseband functionality across a smaller number of sites across the telco’s network and cloud.
CU	Centralized unit
CVP	Core value proposition
DC	Data centre
D-RAN	Decentralized RAN
DSS	Dynamic spectrum sharing
DU	Distributed unit
E2E	End to end
eCPRI	Enhanced common public radio interface
eMBB	Enhanced mobile broadband
EPC	Evolved packet core
EPS	Evolved packet system
ETSI	Organization for European Standards
FWA	Fixed wireless access
GAFAM	Google, Amazon, Facebook, Apple and Microsoft
GSMA	Groupe Speciale Mobile Association
HW	Hardware
IoT	Internet of Things

MANO	Management and network orchestration
MEC	Mobile edge computing
MIMO	Multiple-in, Multiple-out
mMTC	massive machine type communication
mmWave	Millimetre-Wave
MNO	Mobile Network Operator
MR	Mixed Reality
NaaS	Network as a Service
NEP	Network Equipment Provider
NFV	Network function virtualization
NFVI	Network function virtualization infrastructure
NR	New radio
NSA	Non-standalone
OPEX	Operational expenses
Open RAN	Disaggregated RAN functionality built using open interface specifications between elements. Can be implemented in vendor-neutral hardware and software-defined technology based on open interfaces and community-developed standards.
O-RAN Alliance	O-RAN Alliance is a specification group defining next-generation RAN infrastructures, adhering to the principles of intelligence and openness.
OSS	Operations support system
QoS	Quality of service
RAN	Radio Access Network
RCP	Rakuten Communications Platform
RIC	RAN Intelligent Controller
RFP	Requests for proposals
RRH	Remote radio head
SA	Standalone
SDN	Software-defined networking
SMF	Session management function
TCO	Total cost of ownership
TIP	Telecom infra project
UL	Uplink
UP	User plane
URLLC	Ultra-reliable low latency communication
vBBU	Virtual baseband unit
vCU	Virtual centralized unit
vDU	Virtual distributed unit
vEPC	Virtual evolved packet core
VM	Virtual machine

VNF	Virtual network function
VoNR	Voice over new radio
VR	Virtual reality
vRAN	Virtual RAN: an implementation of the RAN in a more open and flexible architecture which virtualizes network functions in software platforms based on general purpose processors.

1. Introduction

5G is one of the key technologies and infrastructure for the industrial and digital transformation. It offers a range of new services and applications for several industries. The development and diffusion of 5G are driven by several technological developments, in which a disaggregation of hardware and software, as well as network function virtualization and containerization, are key trends that allow for radical architectural changes across mobile network domains.

The importance of 5G infrastructure, its fast roll-out and technological capabilities, as well as the development of the supply side of 5G infrastructure, has been highlighted by the European Commission in various initiatives and strategies including the Communications “5G Action Plan for Europe" and “Secure 5G deployment in the EU: Implementing the EU toolbox”. The European Commission also considers 5G as one of five priority areas for standard-setting measures.

However, although Europe is home of two of the three major equipment suppliers and leading in trial investments in 5G, overall infrastructure investments lag behind other regions and Europe’s vertical industries are only just starting to cooperate with network operators to identify valuable 5G business cases. Network operators are confronted with decreasing profit margins and strong competition, while European equipment providers need to sustain their competitiveness.

The objective of this study is to provide the Commission with an in-depth analysis based on qualitative and quantitative information on the 4G and 5G equipment and services supply market trends.

Based on relevant and plausible future-oriented scenarios determined by factors such as evolving technology, standards readiness and RAN disaggregation initiatives, the study analyses the impact on the 5G equipment and services supply markets, and new deployment and operation models.

Finally, the study identifies potential policy options facilitating possible developments and fostering healthy competition for European companies and SMEs in the evolving ecosystems.

In the first phase of the study, a baseline assessment of the 5G equipment and services supply markets including new deployment and operation models, was developed. In this baseline assessment, an analysis of the current state of play of the 4G and 5G supply chain and the market shares of infrastructures providers in the EU and worldwide was performed. The findings were presented and discussed at a stakeholder workshop in December 2020.[11]

In the baseline assessment, we also analysed the status of initiatives that work on the disaggregation of 4G and 5G New Radio (NR) radio access networks (RAN). We investigated the current state of play in standardisation, followed by the most promising and matured Open RAN[12] initiatives specifying the APIs for interfaces and logical splits of the 5G NR RAN defined by the 3GPP in Release 15. Thereafter, we looked into the 4G/5G deployments already conducted towards advancing Open RAN. The results of this analysis are provided as a stand-alone background report to this study.

This final report departs from the baseline analysis, presents results from the scenario analysis and derives potential policy options. Based upon a selection of key trends, which were deemed to be particularly relevant for the future development of the 5G supply market but associated with very high levels of uncertainty regarding the outcome, the study team elaborated hypothetical but plausible scenarios for the future development of the 5G supply market with a time horizon of 2030. The four scenarios illuminate potential pathways for Europe based on different configurations of key technological, economic, social and political factors.

11 The full analysis of the baseline assessment can be found here: https://zenodo.org/record/4621102/files/5GSupplyMarketTrends_BaselineReport.pdf?download=1
12 The term "open‟ in Open RAN refers to the subdivision of network blocks into subcomponents through the definition of new interfaces. However these subcomponents can be built out using anything from open-source to proprietary technology.

As outlined by the Terms of Reference of the study, the four scenarios consider the potential impacts of the increasing virtualization and disaggregation of networks, which may affect not only the current but also future potential equipment supply. The scenarios consider different possible outcomes of developments, in which the 5G industry is moving from a hardware-centric to a software-centric model, and in which hardware could become mostly a commodity. As a result, software and virtualization could lead to a stronger differentiation on functionalities and performance, which may promote the flexibility and scale of 5G deployment and operation.

The subsequent impact analysis for the four scenarios is based upon a review of recent academic literature, market analyses, and more than thirty expert interviews with high-level representatives from Mobile Network Operators (MNOs), vendors, standardisation organisations and relevant associations. This approach comes with certain implications and restrictions of importance to note when reading this report:

- For assessing the impacts of the scenarios, we used nine impact dimensions covering economic, technological, environmental and societal domains; we asked experts to assess each of these domains in the context of the four scenarios.
- Where possible, uncertainty related to quantitative projections included in the scenarios was accounted for. However, underlying data and assumptions for many projections are proprietary or unavailable for other reasons, therefore these data and any associated assessments were not included.
- For some impact dimensions, involving experts to provide independent, objective assessments was not possible, as all stakeholders have some form of vested interest in the future of 5G. This is a common limitation of the available time and method (i.e. expert assessment) chosen.
- While each scenario presented is deemed plausible, it is important to stress that no single scenario in this report is intended to offer a preferred or desired future. Each scenario comes with certain risks and opportunities for Europe. We also stress that the scenarios and impact analysis presented in this report do not represent projections or forecasts: rather, they reflect alternative plausible futures of the 5G supply market for the time horizon of 2030.

The scenarios, informed by diverging opinions regarding the potential direction of highly uncertain trends, have been designed to support dynamic policy responses to the fast-changing future landscape of the 5G supply market.

The high plausibility of the different scenarios was highlighted by the independent expert panel discussion in the second stakeholder workshop performed on 19 May 2021, which served to disseminate, discuss and validate findings of the study on the 5G supply market trends. The workshop was open to all stakeholders interested in the development of the 5G supply market. Overall, 227 interested stakeholders participated in the workshop, offering us further feedback and suggestions to augment the policy options presented for the future development of 5G. Furthermore, an additional expert workshop with a selected number of experts was held on the same day. It created a forum to discuss and further elaborate these policy options against a background of possible long-term development pathways of 5G and beyond. More than 40 invited experts from 5G equipment providers, mobile network operators, standardisation bodies, representatives of vertical industry, and academia participated in this workshop.

This final report proceeds as follows: We first provide an overview of the major trends and drivers influencing the future development of 5G supply markets. Subsequently, we explain the scenario development process and present the four 5G development scenarios. For each hypothetical scenario, we then provide an analysis that addresses nine impact dimensions, covering relevant questions from an economic, competition, regulatory, security, environmental, technology and innovation policy perspective. Based upon the analysis performed, the final sections of the study provide policy recommendations and conclusions.

2. Scenarios for the development of the 5G Supply market

Scenarios are plausible and coherent images of the future but do not have the ambition to predict or forecast the future. They organise multi-dimensional and complex information about future possibilities into comprehensible stories on how the future may look. By mobilizing various experts who are involved in the scenario development process, it is possible to gain a better understanding of the factors that will help to shape the long-term development and future.

Scenario development is a widely used approach by private and public actors. Scenario development is particularly useful in times of high uncertainty and complexity, as is the case with the 5G market. In the past, large companies, young entrepreneurial firms, supranational bodies and policy makers have used scenario development for a wide area of questions often concerning technological development.

To develop the scenarios, we first identified important trends and drivers for the possible development of the 5G supply market. These trends and drivers were subsequently assessed by the research team and using an online survey among experts. Based on this assessment, we identified eight key trends to developed four draft scenarios, which were further elaborated and validated within a workshop held in December 2020. Based on further consultation with experts and stakeholders the scenarios were validated and further refined. See Figure 1 for the scenario construction process.

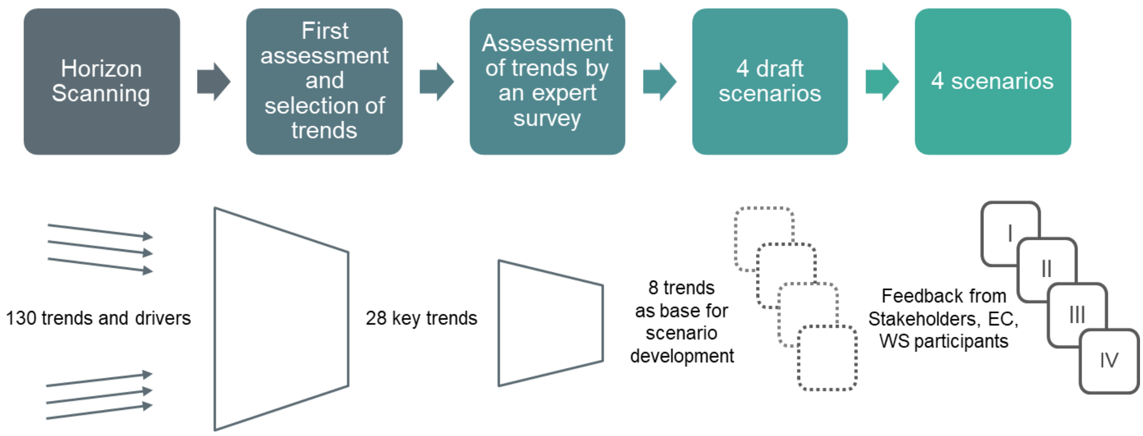


Figure 1: The scenario construction process

The following sections outline the different steps and outcomes of the scenario development in more detail.

a. Major trends and drivers

The basis of the Horizon Scanning activity was a comprehensive screening of foresight reports, business, industry and policy reports, and scientific literature for trends and drivers influencing the future of 5G supply markets. To ensure a coherent approach in the project, the baseline analysis on supply market trends and the status of open initiatives served as a starting point in the search for relevant trends and drivers.

Our analysis identified 130 factors which were then structured according to a STEEP (society, technology, economy, ecology, policy) scheme. The Horizon Scanning approach went beyond the beaten path and initiated an interactive online brainstorming and a discussion of trends and drivers with experts of the project team. The process evoked fruitful debates: it was noted that the main part of identified trends and drivers concerned only three clusters, namely the political, technological and economic cluster, whereas the societal and environmental cluster remained sparsely filled.

Through the Horizon Scanning activity and analysis of results, we identified 28 major trends that significantly influence the future of 5G supply markets. This section presents the set of future-relevant trends and drivers that also served as the basis of the online survey detailed in section 2.2.

Societal trends

Development of use cases in Europe

Use cases drive the commercialisation of 5G. A distinct “killer application” could prove the core value of 5G and raise societal awareness. However, business use cases have not yet been fully explored in Europe; the time and effort used to find the right use cases, especially for verticals, should be considered.

Digital security of 5G networks

A high level of cybersecurity of 5G networks will be needed to ensure secure services for consumers, business and vertical industries. The EU toolbox for 5G security provides a set of robust and comprehensive measures for an EU coordinated approach to secure 5G networks.

Development of data traffic

The last decade has witnessed a never-ending growth in global mobile data traffic; compared to the entire global Internet traffic in 2005, data volume in 2021 is expected to show a 23-fold increase.

By 2023, over 70% of the global population will have mobile connectivity.[13] The total number of global mobile subscribers is expected to grow from 5.1 billion (66% of the population) in 2018 to 5.7 billion (71% of the population) by 2023. 5G devices and connections will be over 10% of global mobile devices and connections by 2023. By 2023, global mobile devices in operation are expected to grow from 8.8 billion in 2018 to 13.1 billion by 2023 – 1.4 billion of those will be 5G capable. The fastest-growing mobile device category is M2M followed by smartphones. The mobile M2M category is projected to grow at a 30% CAGR from 2018 to 2023. Smartphones are projected to grow at a 7% CAGR within the same period.

According to the latest GSMA report, consumer adoption of 5G may reach 20% of global mobile connections by 2025. That said, adoption rates are likely to be higher among countries at the forefront of 5G: the U.S., China, South Korea, Japan, the Gulf states, Australia and parts of Europe[14]. However, in particular for Europe, some experts argue that in the consumer market, growth expectations are rather modest. [15] Europe still has capacity on 4G networks and consumers may not require a faster connection.[16]

Citizens’ concerns on environmental and health effects

Citizens' concerns about 5G revolve around the impact that the higher network frequency could have on humans and animals, such as the potential effects of 5G spectrum mmWaves on insect behaviour and heat regulation.[17] Also, aspects of energy consumption and efficiency of 5G are considered. The EC takes citizens’ concerns on environmental and health issues very seriously and works with the Member States to inform citizens of the strict EMF limits in place. Active monitoring of potential health risks is ongoing (e.g., through revision of the global guidelines for exposure limits).[18]

Education and training to counteract lack of professionals

A shortage of skilled ICT workers could slow down the take-up of 5G as this may hinder the advancement of new services and business models.

13 https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
14 https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=58621970&file=141220-Global-Mobile-Trends.pdf
15 Taga et al. (2021)
16 In the survey we have asked the experts to assess whether a slow uptake is also plausible.
17 Kastenhofer et al. (2020)
18 5G Observatory 2020

Technological trends

Open and interoperable 5G network solutions

The virtualization of the RAN and the development of new RAN architecture (full virtualization of the native 5G core network, Open RAN) are blazing a path for the implementation of open and interoperable solutions in the network.[19] Several initiatives have applied an "Open RAN" model, aiming to replace closed architectures linking proprietary networking hardware and software with more open and modular interfaces.[20] Open and interoperable 5G network solutions could provide an opportunity for new players to enter the RAN market, fostering vendor diversity and increasing the development speed and competition.[21] While open and interoperable network solutions offer notable benefits, trade-offs in terms of performance, costs, energy efficiency, cybersecurity, supplier diversity and reliability remain areas of active controversy among the 5G community and in the literature.[22]

Security challenges in 5G networks

As part of a series of digital industrial transformations, 5G networks will become an increasingly critical infrastructure for the functioning of public and private sectors. With such expected growth, security challenges are likely to grow in prominence as well[23]. These challenges include threats to the availability and integrity of networks, increased exposure to attack, and high-risk exposure of critical suppliers in the 5G ecosystem.

Spectrum availability for 5G use

"Availability of spectrum in low, mid and high bands is key for 5G."[24] In Europe, the 3.4-3.8 GHz band is becoming available early as primary band; spectrum availability will greatly contribute to the position of EU Member States in the 5G arena.[25]

Vertical-specific interoperability aspects

Special attention on verticals is needed due to vertical-specific interoperability aspects which is a prerequisite for many new applications and services, e.g. related to automated driving or industrial automation based on IoT.[26]

Universal standards and open specifications

3GPP specifications and releases along with standard-essential patents (SEPs) could further speed up agreements on universal standards and increase interoperability. Universal standards could in turn open up the supply market landscape to smaller hardware and solution providers or start-ups and promote the diversity of players in the 5G supply market.

Conditions of standard-essential patents licensing related to 5G

Access and pricing conditions of licenses for patents (SEPs) are essential for the implementation of 5G. Standardisation organizations often require licences of essential patents to be on fair, reasonable, and non-discriminatory (FRAND) terms.

Economic trends

Different development paths in global regions

As telecommunications is a global sector, 5G deployment affects all countries. However, in different socio-economic contexts, this trend does not necessarily lead to fair competition and improved geopolitical cooperation in general. Declining investment flows and technology constraints between China and the US already point to reduced dependence.[27] The Covid-19 crisis accelerates the progressive deterioration of geopolitical relations.

Development of vertical markets and industries

19 Pujol et al. (2020b)
20 Plantin (2021)
21 Pujol et al. (2020b); Hofer (2020)
22 See for instance Barford (2021)
23 European Commission (2019)
24 Pujol et al. (2018, S. 28)
25 Pujol et al. (2018)
26 5G Observatory (2020)
27 World Economic Forum (2020)

Developments of 5G application possibilities in vertical markets and industries has implications for future 5G supply markets. Ongoing and profound digital transformation of vertical industries, such as health and healthcare, industry 4.0 and manufacturing, automotive and transport, AR&VR&MR and mining, could create a transformational level of demand for 5G supply. Along with the development of vertical markets and resulting novel 5G use cases, the creation of private 5G networks offers another important new revenue stream for incumbent network operators, vendors, and possible new integrators.

Along with the development of vertical markets and new 5G use cases, the creation of private 5G networks offers an important new revenue stream for incumbent network operators, vendors as well as new integrators. The creation of new revenues is a key motivation of network operators for network overhaul. However, as much as private wireless networks could drive new operator revenues, the opposite could also come to fruition should enterprises wish to build and/or operate their own networks in, for example, industrial campus or factory settings.[28] The latest 5G observatory report indicates that private 5G networks are a highly dynamic market under formation, in which vertical industries, incumbent and new vendors and mobile network operators are taking on new roles.

Network infrastructure sharing

Agreements between MNOs or increasing independent asset infrastructure owners or neutral hosts to share network infrastructure (buyouts, carve-outs/spin-offs of antenna portfolios, etc.) have a great impact on competition. Next to economies of scale and the possibility of lowering increasing investments, network infrastructure sharing could render 5G supply markets more attractive to new players for decreased entrance barriers. The degree and method of infrastructure sharing vary from country to country depending on regulatory and competitive climate.

Risk of falling behind in infrastructure investment and deployment

The current gap in 5G infrastructure deployment in Europe (10 5G base stations per million people in Europe compared to 500 5G base stations per million people in South Korea) increases the risk of falling behind in infrastructure investment and deployment worldwide. This risk exists not only for Europe but also for the US, which could create a $1 trillion global gap in telecommunications infrastructure investment by 2040.[29] This trend could intensify with the observed increase in infrastructure costs.

Increased risk of major dependencies on the complete 5G supply chain suppliers, from component to services

Dependence on a single supplier increases the risk of a possible interruption in supply, resulting for example from commercial failure. It also exacerbates the potential impact of weaknesses or vulnerabilities and their possible exploitation by threat actors, especially when the dependency involves a supplier that poses a high risk.[30] Europe has identified high technology dependence e.g. on components and cloud.

Commercialisation of 5G services

More than half of the EU Member States have not yet launched commercial 5G services, while the first commercial services were available in South Korea and the US a year ago.[31] This trend is also reflected in the deployment of infrastructure (applying to both, migration from 4G to 5G access infrastructure and construction of standalone 5G access infrastructure). A heterogeneous regulatory landscape and varying deployment costs across Europe hamper the speed of commercialisation.

28 GSMA (2020).
29 World Economic Forum (2020)
30 NIS Cooperation Group (2019)
31 ERT 2020a; 5G Observatory 2020.

Deployment costs

The costs of deploying 5G networks require significant up-front investment and depend on the technology mix used, the geography of the country and the population density in each area of the country (i.e. urban, rural or remote areas).[32] In addition, cost-effective spectrum allocation and a sound investment climate are crucial for an effective 5G roll-out in Europe. A challenge for 5G deployment is the structure of the European market, which is highly fragmented;[33] deployment costs vary widely across EU countries.[34] The CapEx/EBITDA ratio remains flat for European operators, while the ratio in the US and South Korea has fallen.[35] At the national level, 5G deployment has also been slowed down by the procedures for obtaining planning and construction permits, indicating a heterogeneous landscape of regulatory frameworks.[36]

5G business ecosystem changes

5G business ecosystem changes depict how 5G networks and related services could unfold over time considering the regulatory changes, business opportunities and technological innovations. The changes primarily concern the performance of players in a future 5G supply market, but also consider different connectivity, context, and commerce business models.[37]

Emergence and entry of new players

Open and interoperable network solutions are paving the way for new players in the 5G supply market. While Open RAN may set enabling conditions for new network vendors, it is not a singular feature driving emergence or entry. New entrants may emerge from established companies with strong competencies in hardware, baseband provision, or software services. In addition, new key players may also emerge from start-ups or other sectors.

Departure of established players

Difficulties in technology development can also lead to current players withdrawing from the market, see the example of Intel.[38] The withdrawal of key players could also affect existing partnerships and development agreements and change the 5G supply ecosystem.

Environmental trends

Energy efficiency

Newer generations of wireless technologies will consume less energy than earlier ones (e.g. 5G antennas will consume less than 4G antennas) (European Commission 2020). In addition, energy-saving processors are expected in the future, which could contain the growing energy consumption of digital technologies by processing data closer to the user, by applications related to IoT and by reducing network latency.[39] 5G will enable more precise targeting of power consumption and a better appropriation of power consumption to actual usage.[40] The development of energy efficiency is strongly related to the question to which extent Open RAN architectures are deployed. While Open RAN offers flexibility, the use of off-the-shelf hardware amongst others comes with a price concerning energy consumption.

Environmental impact

The future environmental impact of 5G is highly uncertain. On the one hand, 5G could offer opportunities to protect and preserve the environment, e.g. 5G with IoT in the context of smart cities could help to increase energy efficiency, reduce greenhouse gas emissions and enable the

32 OECD (2019)
33 ERT (2020a)
34 5G Observatory (2020)
35 ERT (2020a)
36 ERT (2020b)
37 Moqaddamerad et al. (2017).
38 Pujol et al. (2019)
39 European Commission (2020)
40 5G Observatory (2020)

use of renewable energy (microgrid integration), through more efficient and sustainable city management. On the other hand, 5G might harm the environment through increased energy consumption and emissions due to the rising number of global mobile subscriptions and IoT devices, as well as life cycle impacts, i.e. mining and metal processing, oil extraction and petrochemicals, manufacturing and intermediate transports, public works (infrastructure) and power generation with coal and gas, e-waste.[41]

Policy-related trends

Geopolitical conflicts

A reconfiguration of the geopolitical landscape can be observed: geopolitical conflicts, lack of trust, national security concerns, or 5G viewed as an opportunity to (re)build an indigenous industry, may lead to bans of certain suppliers, to a push for disaggregated solutions or new trade tariffs/limits. The Covid-19 crisis accelerates the progressive deterioration of geopolitical relations. The geo-political influence of Europe will depend on its ability to adapt to changing conditions.

Bans on vendors

As telecommunication networks are critical infrastructure, security challenges in 5G networks are also high on the political agenda. While some countries have banned certain vendors right away (e.g. the United States), the EU has chosen a more systematic approach. The EU Member States performed a national risk assessment in 2019 and following these results, the EU 5G Toolbox of mitigating measures and plans was published on 29 January 2020.[42] The Toolbox contains a set of Strategic and Technical measures, aimed at mitigating the main cybersecurity risks of 5G networks.

Among other aspects, the toolbox recommends to assess the risk profile of suppliers and apply relevant restrictions for suppliers considered to be high risk - including necessary exclusions to effectively mitigate risks - for key assets defined as critical and sensitive in the EU coordinated risk assessment (e.g. core network functions, network management and orchestration functions, and access network functions); The toolbox sets out that each operator has an appropriate multi-vendor strategy to avoid or limit any major dependency on a single supplier (or suppliers with a similar risk profile). This includes the promotion of greater interoperability of equipment.

A ban on vendors could slow down the roll-out of 5G if it is not implemented consistently across the EU and appropriate transition periods are not granted. However, considering and dealing appropriately with high-risk providers is crucial for all future developments.

Recent actions taken in many EU Member States are not entirely aligned. Severe restrictions for certain vendors are becoming reality in several EU Member States, which include Italy, France, Finland, Sweden, and Poland although with different modalities and scope on the restrictions.[43] The German government is planning tougher oversight of telecoms network vendors that, while not imposing an explicit ban on Huawei, will make it harder for the Chinese company to keep a foothold in Europe’s largest market.[44]

In a global context, the exclusion of players could affect existing technological path dependencies and deteriorating geo-political relations. Most experts argue that a ban on vendors and the possible change of equipment providers is associated with higher cost and that a ban on suppliers could slow down the introduction of 5G solutions, in particular if no adequate transition periods are allowed.[45],[46]

---

41 See e.g. Ercan (2013)

42 Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, 29 January 2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

43 See: https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/2/

44 Source: Reuters, September 30, 2020.

45 Taga et al. (2021).

46 However, some recent examples reveal that a change of vendors not necessarily is associated with higher costs (https://www.lightreading.com/5g/belgian-telcos-drop-huawei-for-nokia/d/d-id/764525).

To alleviate this threat, countries like Japan, the United States and the United Kingdom are making national budgets available to support operators replacing high-risk vendors with other solutions.

Heterogeneous European regulatory landscape
The regulatory framework in Europe is crucial to the further development of 5G supply markets. For example, slow procedures for obtaining planning and construction permits slow down deployment and increase deployment costs, whereas regulatory incentives could drive investment and innovation in 5G.[47]

Degree of pan-European cohesion and scale in public initiatives
Government 5G investments in Europe have historically occurred on a national level, creating a challenging environment for achieving pan-Europe public initiatives with high cohesion and at scale. While some European states have launched and are progressing national 5G programmes of variable size, others lag behind.[48] Existing small-scale programmes at the national level focus on research and piloting rather than broader implementation across Europe. Recent active guidance from the European Union, including the 5G Infrastructure Public-Private Partnership (5G-PPP) and the Joint Undertaking on Smart Networks and Services towards 6G (SNS JU) proposal, is beginning to address this challenge.[49] The European 5G-PPP represents a leveraged 3.5 billion Euro investment in 5G of which €700 million is public investment.[50] The SNS partnership proposal has an earmarked public funding of €900 million to be matched by the private sector by at least the same amount.

Technology neutral regulation
Technology neutral regulation aims at the promotion of competition between different technology solutions and at regulation that does not back any particular technology but enables technological solutions irrespective of a particular business model or application.

Increase public R&I investments for EU players
Current European R&I investment in 5G development is low by international benchmarks (APAC).[51] Increased R&I investment for European players could help the 5G innovation ecosystems thrive.

Policy support for new actors
Funding and financial support for new players entering the 5G supply market could help facilitate 5G deployment and increase the diversity of European 5G supply market actors.

b. Assessment and selection of trends and drivers

To develop scenarios, different trends have to be selected and integrated into coherent pictures of the future. Following the approach described by Schoemaker (1995), we selected and assessed the previously identified trends and drivers based on a two-step process. First, we conducted an internal workshop (with members of the project team) and selected 29 from the total list of 130 trends and drivers.

Second, we conducted an online survey to assess experts' perceptions of the impact and uncertainty to select trends and drivers for the construction of the scenarios. The purpose of the expert survey was to assess the impact of various trends and drivers on the potential evolvement of the 5G supply market. In addition, the respondents were asked to assess their confidence in their assessment. The corresponding survey questions for each factor were:

47 See ERT (2020b) and the European Electronic Communications Code https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972 .

48 Taga et al. (2021, S. 12)

49 See the SNS proposal: https://digital-strategy.ec.europa.eu/en/news/europe-puts-forward-proposal-joint-undertaking-smart-networks-and-services-towards-6g.

50 Taga et al. (2021, S. 12)

51 Taga et al. (2021)

- How do you assess the future impact of the following factors on the development of 5G supply markets in Europe until 2030? (scale: no/very little impact, some impact, strong impact, very strong impact)
- How certain are you that this development will become reality? (scale: uncertain, certain)

The survey was conducted online in November 2020. Over 500 experts from different organisations were contacted for the survey. The geographic scope was concentrated on Europe (including non-EU countries) but also considered overseas experts' views to capture a broader field of perspectives. The group of experts contacted included managers, researchers, representatives from intermediaries, foresight experts and policymakers. In the survey period from 23 November to 9 December 2020, we received 53 complete responses from experts, who assessed 28 key factors in the five dimensions (Society, Technology, Economy, Environment, Policy).

Figure 2 gives an overview of all trends and drivers assessed according to the impact they would have by 2030 and according to the uncertainty that this trend will take place until that time.

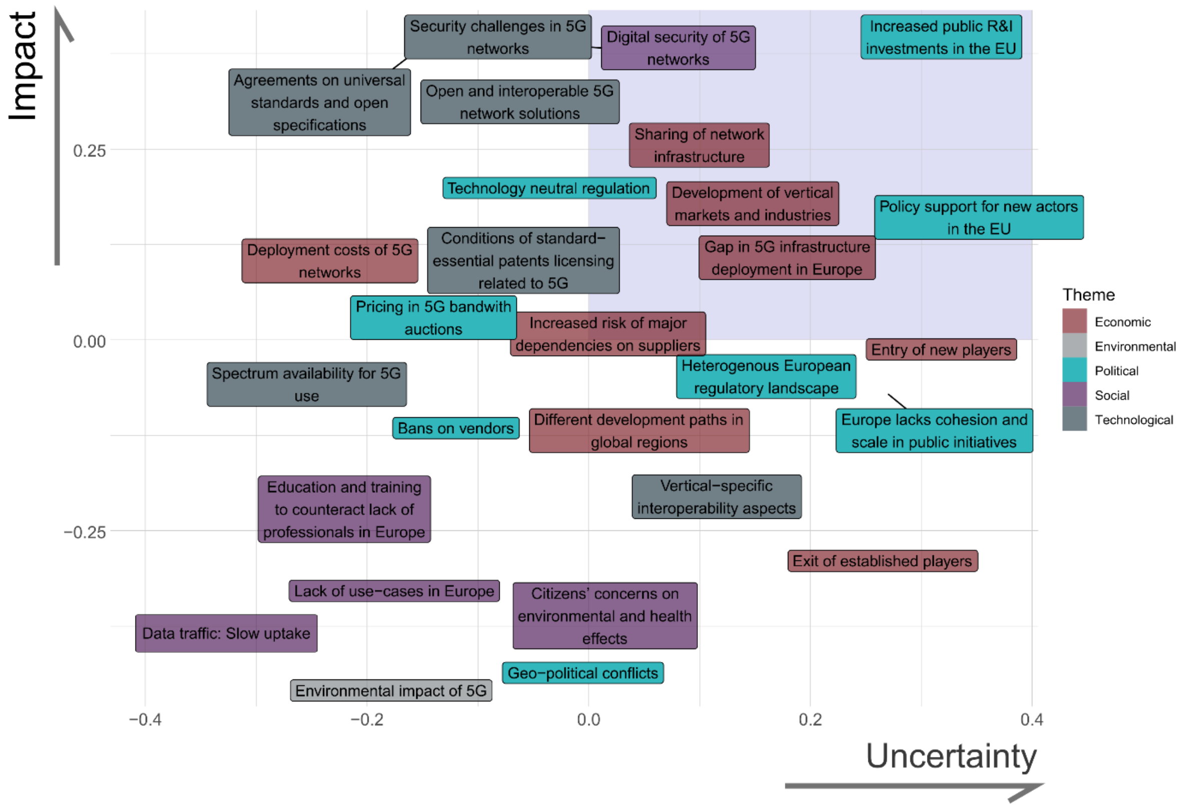


Figure 2: Assessment of trends and drivers[52]

Figure 2 consists of four quadrants: Quadrant I (bottom left corner) shows what respondents estimated to have the lowest uncertainty and the lowest impact. These results can usually be neglected for the scenario building because if in the unlikely case that they occur, they will not have a noticeable impact, at least not until 2030. Quadrant II (top right corner) displays the trends and drivers with the highest estimated impacts and the highest uncertainty to take place. These factors are the most interesting trends and drivers for the construction of the scenarios in the subsequent steps of the study. If they occur, they might have a very big impact. Next, quadrant III (right down corner) displays the trend and drivers with the highest certainty and the lowest impact. They are sometimes taken for scenario construction, but often, they are taken care of by policy-makers, so there is less need to point to these trends and drivers. Lastly, quadrant IV contains

52 Normalised average responses to the assessment of the factors' future impact and uncertainty of development. Normalised answer categories are mapped with a mean of 0 and standard deviation of 1 as follows: No/very little impact (-2.2), Some impact (-1.0), Strong impact (0.1), Very strong impact (1.3); No/very little uncertainty (-1.2), Some uncertainty (0), Strong uncertainty (1.2), Very strong uncertainty (2.4).

trends and drivers with the highest uncertainty and the highest impact. So, these factors will most likely have an impact in the future.

c. Construction of scenarios

Based on the ranking of trends we selected eight trends (mainly those with a high impact and at the same time a high uncertainty) for the construction of a set of scenarios integrating factors from different dimensions. These eight key trends were:

- Open and interoperable 5G network solutions
- Entry of new players
- Development of vertical markets and industries
- Increased R&I investments in the EU
- Level of EU cohesion
- Policy support for new actors in the EU
- Security challenges in 5G networks
- Universal standards and open specifications

To construct a limited set of coherent plausible scenarios we conducted a morphological analysis.[53] Within a morphological grid for all factors (trend and drivers) selected the possible projections are given. We performed a consistency analysis to test the plausibility of possible combinations. The four scenarios result from an individual combination of all factors considered. See the following table for how the different factors have been combined into the different scenarios. Each trend can have a slow, moderate or high/rapid development speed and some relevant developments are described briefly.

Key trends	**Scenario I: Incumbent players driving 5G**	**Scenario II: Slow pace of 5G Roll-Out**	**Scenario III: Open RAN as a game-changer**	**Scenario IV: 5G for Big Tech**
Open and interoperable 5G network solutions	Moderate Proprietary RAN networks dominant, open interfaces are used for specific applications and in some areas (e.g. greenfield investments). MNOs invest in vRAN and Cloud RAN as an intermediate solution. Customer demand serves as an important pull factor for the development.	Slow MNOs are slowly starting to migrate to 5G Open RAN networks, mainly in suburban and rural areas, interoperability is not fully achieved. However, the slow diffusion of open and interoperable 5G network solutions is essentially not the cause for a slow 5G roll-out in Europe.	Rapid Open and fully interoperable standards-based equipment and network infrastructure is rendering multi-vendor interoperable end-to-end networks available, in urban and rural areas. Open 5G innovation platforms are thriving the 5G supply market ecosystem with a strong focus on Open RAN products with potential for radical innovation, however, this is a development with a longer time perspective and will not be realised before 2025.	Rapid Cloud RAN solutions are broadly introduced, open 5G innovation platforms facilitate digitization among industries. Big Tech companies are driving open standard development, though for some interfaces open standards are still not available. Open specifications drive investment by relevant players.

53 See for instance Johansen (2018).

Entry of new players	Low MNOs are using existing vendors but also gradually integrate new suppliers by building up system integration capabilities.	Low European equipment suppliers are preferred through regulation (public procurement) and public R&I investments; new European players are slowly emerging.	High Move from monolithic/single vendor telecom network infrastructure to open cloud and software-based IT solutions. New players widening the industry through broad deployment of small cell networks. While there will be many new entrants from the US and Europe in the short and medium-term, consolidation will happen in the longer term.	Moderate New, often large players enter the supply market and act as the new virtual operators and drive standardisation processes, many European players (especially smaller companies) drop out of the supply market.
Development of vertical markets and industries	Moderate Due to the growth of verticals, MNOs have the willingness to invest	Low 5G-based industrial services only emerge slowly.	High New entries serve the needs of verticals	High Big Tech companies push the development
Research & Innovation (R&I) investments in the EU	High R&I investments important to assure framework conditions for orchestration and interoperability. R&I investments concerning 3GPP standardisation processes are substantial.	Low R&I investments are dedicated to the harmonisation of regulatory frameworks and to support a broad 5G roll-out.	Moderate R&I investments are focused on tailoring 5G networks and services to specific societal needs, as well as integrating new technologies (e.g. Artificial Intelligence/Machine Learning). Venture capitalists and verticals are investing in new entrants.	Moderate High share of private R&I investments (Big Tech companies, verticals)
Level of EU cohesion	High The 3GPP roadmap guarantees the cohesions between national deployments. Many European countries have launched national 5G R&I programmes, though the scale of the programs varies from country to country.	Low Government investments in Europe have tended to be on a national level, and there has been little guidance or direction from the European Union. Several European countries exclude specific equipment suppliers.	Moderate The need for coordination among the European Member States to support Open RAN deployment is modest.	High Cross-border coordination is in place, harmonisation across Europe is driven by new Big Tech business models and use cases that are taken up by EU policies. This leads to 'cherry picking' of urban areas for Open RAN-based 5G deployment (as data collection is driving Big Tech).

Policy support for new actors in the EU	Moderate Support of a heterogeneous 5G supply market ecosystem, supporting new players, that enable digital transformation; global conflicts are mitigated.	Low Though some European newcomers are emerging, policy support is limited and dedicated to the further roll-out of 5G Open RAN networks in rural areas.	High Policy encourages innovation along the entire supply chain through competition	Low Minor policy support for verticals in terms of informing on cost-sharing models, monitoring KPIs, securing basic services, reducing environmental impact.
Security challenges in 5G networks	Low MNOs and established vendors have the capabilities and experience to cope with various cybersecurity issues with the 5G toolbox serving as an important instrument.	Low Despite the existence of the 5G toolbox, only a fragmented approach to the implementation of cybersecurity requirements is realised.	Moderate New and innovative solutions sometimes reveal new vulnerabilities and security loopholes in 5G Open RAN environments.	Moderate Big Tech companies guarantee for security of 5G networks but do not disclose security matters. Security requirements that are enshrined in law.
Universal standards and open specifications	3GPP Open RAN specifications 3GPP Open RAN specifications are used to build up a 5G supply ecosystem by incumbent MNOs and vendors; European players contribute in further developing standards for interoperable multi-vendor end-to-end network functions.	3GPP Open RAN specifications 3GPP Open RAN specifications are used to build up 5G Open RAN networks.	3GPP Open RAN specifications and O-RAN Alliance Universal standards and open specifications developed by open-source foundations are in place under an open-source paradigm, also smaller companies and innovative start-ups involved in standardisation processes.	New consortia develop standards New consortia driven by Big Tech companies develop new standards for interoperable 5G innovation platforms which are used to integrate verticals. In the long term, the role of standardisation might erode.

Table 1: Morphological grid for the construction of 5G scenarios[54]

d. Four scenarios for the future of the 5G supply market until 2030 in Europe

Based on the above-mentioned development process, we developed four scenarios which are being presented next.

Scenario I: Incumbent players driving 5G

Key Storyline: Incumbent vendors and MNOs orchestrate the emerging 5G innovation ecosystem

Driven by increasing demand for new services from verticals that require high performance, incumbent vendors and MNOs are shaping the ecosystem. Equipment from providers considered to bear security risks is used outside the core network in non-sensitive areas only. The adoption of Open RAN for specific applications and in specific regions set incentives for established vendors to further improve the efficiency of their proprietary solutions, which allows them to remain competitive in an increasingly competitive market. Incumbent network equipment vendors continue to operate successfully but new equipment providers are emerging, further facilitating network integration and contributing to an increasingly competitive 5G Open RAN environment. Cloud RAN and vRAN are an important intermediate step of MNOs in their investment paths and can fulfil the performance

54 The table reveals the trend velocity indicating the intensity of the change foreseen in the scenario and describes the development of the individual trends in the different scenarios.

requirements in the short and medium-term. In the short run, Open RAN solutions are mainly applied for niches, but Open RAN does not serve as a game-changer.

Scenario II: Slow pace of 5G Roll-Out

Key Storyline: Modest demand by consumers and industries and inconsistent implementation of cyber-security requirements in Europe hampers a fast 5G diffusion

In this scenario, MNOs and vertical industries are struggling to find the right business case for 5G. Consumers are indifferent towards higher broadband speeds offered by highly-priced 5G networks and are served over a wide area with 4G. 5G-based industrial services only emerge slowly. A fragmented approach to the implementation of cybersecurity requirements in Europe leads to legal uncertainty concerning supplier requirements and long transition periods for updated multi-vendor strategies. At the same time, conditions for increasing multi-vendor interoperability of standards-based interfaces are not being reached in the medium term. As a result, 5G deployment in Europe in consumer and business markets is of modest speed. MNOs slowly start providing end-to-end Open RAN networks, primarily in suburban and rural areas, as their performance is below the expectations.

Scenario III: Open RAN as a game-changer

Key Storyline: Decentralized, disaggregated and fully virtualized Open RAN networks serve Europe

In this scenario, it is envisioned that technological progress is impressive and Open 5G innovation platforms enable highly standardised services on fully virtualised networks in the medium and long term. The demand for new 5G services and solutions is created by verticals that are served by MNOs (mobile network operators) but also new entrants specialised in operating networks. Established MNO, incumbent vendors, verticals and new entrants build up the 5G innovation ecosystem and new specific solutions such as private networks for factories or solutions for autonomous driving are on the rise. Open RAN solutions drive suburban offerings at low cost and broaden the range of services also in rural areas. MNOs face competition by both new European and non-European operators who enter the industry to serve specialized areas, which in turn, accelerates the interest by verticals. This leads to an increasing differentiation in customer segments. Strong policy support for pilot projects in collaboration with verticals pushes applications in new fields. 5G supply markets are characterised by high levels of competition. As the need for telecom system integration expertise is high, new players, which offer technology-based innovations for digital transformation, are gaining importance.

Scenario IV: 5G for Big Tech

Key Storyline: Big Tech companies conquer the 5G supply markets with Open RAN business models

Virtualisation of networks and disaggregation of software and hardware change the landscape for network equipment, deployment, and service provision in the long term. The development is changing the definition of “infrastructure” as software can be run on someone else’s physical infrastructure and virtualisation and the use of clouds becomes more commonplace. New business models based on Open RAN architectures and interfaces are gaining momentum and new major players (e.g. GAFAM) are entering the 5G supply market. Complete and operational 5G solutions (from hardware to software) encourage companies from vertical industries to enter the 5G supply market. MNOs (mobile network operators) are not able to find their role as infrastructure providers for industrial players. They are outflanked by Big Tech companies who also offer services to end-users. Big Tech companies become the "new operators" by offering carrier-like services bypassing incumbent mobile network operators. Thus, Big Tech companies will serve as virtual operators.

3. Scenario Impact Analysis

The four different scenarios presented in the previous section describe different pathways for the future development of the 5G supply market. They aim to inform companies, researchers, interest groups, standardisation bodies and policymakers in their decision-making and to facilitate a debate about how to shape the future development of 5G. To support decision-making, an assessment of the scenarios can deliver further evidence for the various stakeholders concerned.

Because different actors and stakeholders of the 5G supply market have different interests and perspectives, we assume that the scenarios have heterogeneous implications and effects for different stakeholder groups. Indeed, impacts go beyond a pure market-based dimension and affect issues such as cybersecurity or energy consumption, which ultimately are of interest to society at large. We, therefore, assess the scenarios against several impact dimensions and take into account perspectives from different market players (e.g. MNOs and equipment vendors) and other stakeholders (e.g. citizens, public policy).

As a result, the assessment of the scenarios delivers more nuanced information about possible firm strategies and policy options. For instance, an actor might choose to develop a strategy based on the most likely scenario ("planned strategy") or to develop a strategy that supports the scenario which best fits the current business or policy goal and at the same time mitigates the risks of other scenarios ("preventive strategy"). A systemic assessment of the scenarios is hence an important step to exploit the results of the developed scenarios.

To assess the impact of the four scenarios, we address the following nine dimensions that have been outlined in the Terms of Reference of this study, covering relevant questions from an economic, competition, regulatory, security, environmental, technology and innovation policy perspective:

- Market Competition
- Costs (CAPEX and OPEX)
- Business requirement and models
- New services and applications
- Modularity and supplier dependency
- Cybersecurity
- Energy efficiency and consumption
- Interoperability: standards needs and licensing issues
- Overall economic impact for Europe

As Open RAN is one of the fundamental **key trends for the future of the 5G supply market** and the development of the different scenarios, the possible development and diffusion of Open RAN was a key element in some assessment dimensions. Thus, Open RAN has been considered as one of the key factors for the construction of the scenarios and has raised much attention within the scenario assessment, too.

For the assessment of the scenarios, we referred to more recently published studies and data about the development of 5G. Moreover, we conducted 30 interviews with representatives from MNOs, vendors, research institutes and standardisation bodies using a semi-structured interview guide. Interviewees were asked to make a distinction between the impact of a scenario from the perspective of the interviewees' organisation and the perspective of the European ecosystem. We explicitly asked about the opportunities and threats for MNOs and vendors as major players in the supply market.

We first provide a synthesis of the scenario impact analysis in a nutshell. We then take a deep dive into the specific assessment dimensions of the impact analysis. Each sub-section contains 1) an analysis of the current situation and sources of impact, and 2) an in-depth scenario-specific assessment.

a. Synthesis of the scenario impact analysis

Based on the evidence and judgements collected, a synthesis of the impact analysis for the four scenarios along the nine dimensions can be made. The synthesis clearly shows several trade-offs, which can be illustrated as follows:

Assessment dimension	Scenario I: Incumbent players driving 5G	Scenario II: Slow pace of 5G Roll-out	Scenario III: Open RAN as a game-changer	Scenario IV: 5G for Big Tech
Competition	The opportunity for MNOs in the context of open interfaces is that their orchestration efforts bring increased competition by attracting entrants However, if few proprietary Open RAN solutions dominate, this could undermine some of the supplier diversity benefits of Open RAN	Market concentration remains the same or even decreases due to vendor bans Market size does not expand due to low uptake of B2B use cases This scenario threatens to lower Europe's competitiveness	This scenario is expected to increase innovation incentives, assuming uncertainties are solved. New suppliers emerge and competition in the RAN domain increases. However, the most plausible outcome is that non-EU entrants lead the take up of the market share subject to be disrupted There is however the threat of re-consolidation in the longer term, which would reverse the expected benefits	Foreign Big Tech companies increase their overall dominance at both the demand and the supply side However, their specific entry to the B2C connectivity and RAN equipment markets may be unrealistic
Costs	There is an opportunity for MNOs to keep the challenging costs of system integration relatively low compared to a scenario where a dominant system integrator appears However, their ability to afford new Open RAN deployments is questioned Lack of scale and innovation may keep OPEX of new solutions high	This scenario resembles the status quo the most, in terms of costs Equipment prices may even increase if competition decreases	Equipment costs (CAPEX) go down due to competitive pressures Innovation is high, and so is the scale of deployments. OPEX of Open RAN deployments catches up and even may outperform traditional ones System integration costs remain a challenge due to increased complexity, bringing high uncertainty to TCO	The impact on RAN-related OPEX is low. Tech companies only take over a small part of a base station's processing However, the higher bargaining power and overall dominance of GAFAM threatens to keep the prices of their solutions high

	compared to current solutions			
Business models and requirements	It seems unlikely that European MNOs have the resources to integrate multiple vendors elements themselves Nevertheless, large MNOs feel confident they have the expertise to do integration research, which assuming coordination, the less costly marketplace model would seem feasible	The slow 5G rollout does not provide opportunities for new vendor solutions to scale The traditional integrated model remains the most dominant one	In this scenario, the system integrator (SI) business model is of high relevance The 'white-box' model based on open-source is most likely to gain pace Traditional vendors maintain the opportunity to take an early lead in Open RAN and make sure new players develop under their leadership	The threat for European MNOs is that foreign Big Tech players become the go-to integration option On the demand side, Big Tech business models based on their cloud and OTT services help GAFAMs increase their dominance
New services and applications	Such a surrounding is conducive to the development and introduction of new services since it offers security and stable relations between MNOs and their retail customers. However, incumbent MNOs with their focus on hardware may not the best actors to introduce new services Services emerge that are a continuation of existing offers rather than radical departures from the existing services	Rapid development and market introduction of new 5G based services seem unlikely in such an environment Moreover, segmented geographical markets may further hamper the roll-out of Europe-wide services when national policy pushes the introduction of 5G, health services benefit; otherwise, lack of performance and diffusion of 5G may hamper health services	High levels of competition and new network operators lead to low prices and a high willingness for experiments in the market More suppliers in the vendor ecosystem allow deployment of customized networks for different user groups, though, with higher risks of network outages due to a more complex environment Interoperability among European countries facilitates the rollout of use cases Such an environment favours new, data-intensive services (e.g. CAM, IoT and health)	Connected and Automated Mobility (CAM) services and applications benefit in particular. Complementary competencies within Big Tech companies also benefits health use cases
Modularity and supplier dependency	Vendor lock-in is reduced as a consequence of a larger set of	Similar levels of modularity cause	Vendor lock-in in the RAN becomes a problem of the past, although with	Vendor lock-in for the RAN is

	supplier options available to MNOs	vendor lock in to persist Potential adverse effects from disaggregation are less likely	a threat of lock-in at the system integration level Higher entrance of smaller players threatens to lower supply chain resilience, due to potential disruptions in case suppliers go bankrupt or are removed due to cybersecurity concerns	substantially reduced However, reliance on large foreign players threatens to bring a new bottleneck in the supply chain (e.g., at the cloud level)
Cybersecurity	MNOs and incumbent vendors invest in risk mitigation and could thus secure market advantages for themselves	Gives more time to reflect on risks and mitigate them May provide telco companies time to remain incumbent actors	While Open RAN may bring more interoperability, it can also exacerbate cybersecurity risks by providing more entry points for hackers, irrespective of vendor. Addressing cybersecurity challenges might delay the diffusion of Open RAN	Big Tech is not necessarily more secure than medium or small tech, but the scale of people reached is likely to be higher.
Energy efficiency and consumption	Incumbent MNOs may be beneficial for energy efficiency because they are incentivized from a cost point of view	Relying on existing networks where there is a sunk cost in terms of manufacturing and carbon footprint may have a beneficial impact in terms of overall energy consumption Single-vendor solutions are generally more energy-efficient due to integration and optimisation	Less centralized oversight of overall energy consumption The more heterogeneous the networks, the more difficult it is to realise power gains More efficient in the medium term for greenfield networks Open RAN may make it more difficult to measure and control energy in each part of the network Open RAN solutions will consume more energy as designed for flexibility and	It may be beneficial for energy reduction because large tech companies already manage energy in data centres although not so significant to the RAN domain as centralization is reduced The future of Big Tech in 5G is not certain given anti-trust and privacy challenges faced

			interoperability not for optimisation and integration For the same performance and speed, Open RAN will need more sites than integrated solutions; consequently, power consumption notably increases	
Interoperability: standards needs and licensing issues	O-RAN specifications complement the RAN standards set by 3GPP MNO opportunities exist by enlarging the supplier base and increased competition, thus reducing the dependency on few remaining suppliers The threat to MNOs is caused by too little acceptance of O-RAN specifications due to reducing the involvement of all stakeholders in the standardisation process	Negative implications for standardisation both at 3GPP and ORAN Alliance due to less feedback from the applications of 5G standards in practice back to standardisation	The O-RAN architecture and its specifications would become (de facto) standards for RAN The O-RAN architecture will attract new suppliers, which might eventually contribute to standardisation both at 3GPP and the O-RAN Alliance Under this scenario, interoperability and therefore standards will become more relevant in general To handle the complexity, MNOs can opt for a subset of suppliers and proprietary implementations of Open RAN solutions	Big Tech companies become dominant also in standardisation; their influence in the O-RAN Alliance might become bigger, reducing the relevance of existing players. However, they could also start offering non-O-RAN proprietary solutions Common open standards and specifications developed under the roof of the O-RAN Alliance allows competition among MNOs in the EU Service offerings by Big Tech firms might be beneficial for customers If the EU MNOs significantly lose market share, in the long run, their influence in standardisation will be reduced
Overall economic impact for Europe	The contribution of 5G will be the same as the current contribution of 4G technology to	The slow roll-out in this scenario may be partly compensated by the favourable	Offers some possibilities (new opportunities for European suppliers, MNOs	Offers possibilities particularly when European players and new entrants

	Europe's economic growth	conditions for European suppliers of 5G equipment. Nevertheless, the negative effects from a delayed roll-out are larger than the positive effects for European suppliers in this scenario	and service firms) but also some risks at the same time (dominance by non-European firms) Quite an uncertainty on the TCO to determine if European MNOs will reduce costs EU vendors risk reducing their market share, although some other opportunities arise (e.g. system integrators)	can exploit the possibilities due to a changing market landscape European MNOs and European vendors strongly threatened

Table 2: Summary of the assessment

During the interviews and workshop organized in December 2020 participants and experts were asked to rank and comment on the likelihood of each scenario; these perspectives are summarized in Table 3, below:

Scenario I: Incumbent players driving 5G	**Scenario II: Slow pace of 5G Roll-out**	**Scenario III: Open RAN as a game-changer**	**Scenario IV: 5G for Big Tech**
High likelihood	Medium likelihood in general	Medium likelihood	Less likelihood in the short to medium term
Best describes the current situation Considered by some experts as the most likely scenario, particularly in the short and medium-term	Considered as plausible short-term development for some countries Some experts even considered this scenario as most likely	Likely in the medium- to long-term, although deemed less so than Scenario 1 Was considered by some experts as rather visionary	Likely in the medium- to long term and for 6G It was considered plausible that big players such as Google or Amazon, not hindered by legacy technologies, enter the market

Table 3: Likelihood of the scenarios

The scenarios have been constructed for the time horizon of 2030. The results of the scenario development and impact analysis highlight the current uncertainty and diverging assessment and expectations regarding Open RAN in the short- and medium- terms.[55] While scenario I and II can be considered as pathways which might become reality on the short to medium term, scenario III and IV can be considered rather as medium and long term pathways. However, they might also run in parallel (e.g. in different countries) or can follow one after the other, e.g. scenario 1 might evolve into scenario III or IV in the long term. Nevertheless, each of these developments and assessments points to actions and innovations that might become more relevant and potent in the future.

Scenario I reflects some ambivalence about the perceived impact of Open RAN on 5G supply markets.[56] On the one hand, high expectations are attributed to the approach, from opening up the supply market to new players to reducing existing dependencies on specific suppliers. On the other hand, they are also the long-established players who are driving the technology design and

55 see Barford 2021; Plantin 2021
56 see Plantin (2021)

standardisation processes and who might in the future be confidently opening the door for the Trojan horse (tech giants).

Scenario II reflects long-term risks for Europe if a set of trends including low levels of innovation in 5G supply markets, increased vendor lock-ins, limited business cases and subsequently low demand for 5G converge in Europe. Scenario II presents perhaps the most significant risks for Europe.

Although deemed less likely in the mid-term, Scenario III represents effective fostering of a diverse, open, and interoperable 5G innovation ecosystem, illuminating the potential of Open RAN to drive progress in terms of interoperability in general, as well as in terms of reducing dependencies in technology. Key risks posed by this scenario include a loss of technological sovereignty and low levels of European added value; undesirable elements for Europe to consider avoiding.

Finally, Scenario IV presents a clear, long-term vision of Big Tech players disrupting the 5G supply market, underlining the role Open RAN could play in a long-term push to drive network function virtualisation.[57] Key risks surfaced in this scenario also include a loss of technological sovereignty and low levels of European added value, undesirable outcomes for Europe.

While the scenarios share a time horizon of 2030, no single scenario was expected to be primary across all of Europe. Indeed, the way the future unfolds across Europe may incorporate elements of each scenario running in parallel (for example, unfolding differently in different countries) or in series (e.g. scenario III proceeding scenario I).

b. Market competition

Current situation and sources of impact

The RAN market has undergone a process of consolidation over the last decade which resulted in mainly three main vendors in the RAN domain: Nokia, Ericsson and Huawei. ZTE and Samsung and others today have together a market share of around 10%.[58] Current geopolitical decisions and cybersecurity concerns limit the viability of Huawei as an option in Europe, restricting the supply side of the RAN market even more. For new players to enter the current market, long-term high R&I investments as performed by Huawei over the past decade would be required. Consequently, European MNOs today are confronted with only two or ‘two and a half’ supply options.

Innovations in the RAN market through 1) network virtualisation, 2) software-defined networking, and 3) network functions virtualization at the networks’ core and edge could contribute to a reconfiguration of the existing market structure as the physical infrastructure might not have to rely on proprietary appliances in the long run: By opening up interfaces in the future, particularly due to the functional split between radio components, new market entrants would have a greater chance to enter the market. The disaggregation could bring a segmentation of the market and facilitate the entry of companies that are specialised in single, discrete elements or applications. For instance, this could mean specialised suppliers of chipsets, infrastructure, the radio module, software, etc. entering the market.

Overall, such a development could disrupt the market and MNOs would have more options, and the decision to integrate new suppliers' products would depend entirely on the MNO. While this trend of disaggregation is not new in the telecommunications industry - for instance, the interface between the RAN and the core network is already standardised and open -, it would represent a novelty in the RAN domain.

A parallel trend that will give opportunities for new entrants to enter the market is the greater importance of B2B use cases: the need to have customised private networks and solutions - for example, by big industry players or automotive use cases - is also expected to increase the

57 see Plantin (2021)
58 See: Taga et. al. (2021)

importance of more specialised services and equipment suppliers, which do not need to consider the full legacy of network solutions based on 3G, 4G, 5G systems.

Finally, market competition will also be heavily affected by policy support. Policy support can foster and hamper the emergence of new national or regional entrants. Recent reported proposals for public funding –see, e.g., those in the US and Germany – exemplify this view. This implies that, beyond technological development, the geopolitical factor also needs to be taken into account when considering the impact of the Open RAN movement on the competition.

Expected outcome and outlook

While the expected outcome of these trends on the market structure might be limited in the short term, experts forecast an increased supplier diversity once the technology matures; in the long term, however, this diverse ecosystem may remain or be reversed to yield a consolidated market such as today.

For the **short to the medium-term** horizon, no major changes in the market structure are yet visible. As of today (first quarter of 2021), almost the entire 5G equipment market is composed of commercial deployments that have not been based on Open RAN. 5G infrastructure deployments are being rolled out at a time before Open RAN solutions are mature. The most optimistic estimates by Open RAN proponents target around 2025 as a point where maturity for high-capacity performance solutions can be reached. Therefore, in the short term, 5G deployments will most likely rely on single-vendor solutions, which are expected to outperform multi-vendor ones. As the lifecycle of equipment for a generation is usually about a decade, operators who have already bought equipment for 5G may not plan a hypothetical switch to Open RAN until the mid to long term. As of today, only a limited number of Open RAN deployments have been deployed[59] and there is only one extensive commercial network based on Open RAN, Rakuten in Japan. Whereas in total, as of March 2021, 5G commercial rollouts reached 158 local operators with active networks in 67 markets[60] worldwide as of March 2021.

However, this does not need to be the case for certain rural areas or sites that rely on private networks: MNOs doing greenfield, or new build, like Rakuten in Japan or new enterprise/campus networks, will see Open RAN as an option sooner than incumbent MNOs will for public networks, because they will not have to deal with all the existing architecture. On the other hand, incumbent MNOs have established subscriber bases and done massive investments in legacy networks supplied by traditional vendors' equipment; hence, they will have to figure out how to integrate new equipment with the existing one, and this will be challenging work which may question the feasibility and/or delay the adoption of Open RAN architectures some few months or years (this integration may be done in-house or outsourced, as discussed within the 'business models' dimension).

For the longer-term horizon of the scenarios, there were divergent views:

- A vast majority of our respondents agreed that Open RAN will lead to more competition amongst vendors once it matures, all else equal. In the mid-term - i.e., on the first years since the mentioned maturity point, expected to be in 3-4 years -, they expect it will expand the ecosystem of vendors and increase competition and product innovation. However, views vary in terms of the extent of entry in the supplier market: while some expect dozens of new entrants to be realistic in the mid-term due to opened architectures, others think the number of players may just double (say, 6-7 in total). The reason for the latter view is that the amount of R&D and investment required to develop competitive radio components and chipsets is significant and will still represent a barrier to entry even in the scenarios where Open RAN is most mature.

59 See Taga et al. (2021), p. 16 for an overview
60 See https://www.spglobal.com/marketintelligence/en/news-insights/research/67-markets-worldwide-have-commercial-5g-services

- Regarding the longer-term (for reference, about 2030, a similar horizon to the scenarios), there were also divergent opinions among those who expect higher competition in the mid-term. Three respondents explicitly doubted the capacity of the market to sustain many players competing in the RAN space. In practice, this would mean that in the longer term, the market consolidates back into a handful of suppliers. The causes of this consolidation can be mergers, acquisitions or the financially unsuccessful ones leaving the market. Traditional vendors or early successful companies may acquire smaller ones (e.g., threatening entrants or those with valuable patents). In this setting, even if new EU start-ups arise, they can be quickly acquired, potentially by big, foreign players. A point of concern is that common reasons to acquire ventures can not only be to integrate their technology but also to erase a potential competitor. In addition, these respondents mentioned that it is hard to predict who will be the remaining players in this consolidated scenario. The remaining players may not necessarily be the traditional ones: a shakeup of the industry is possible, for instance, if Big Tech companies or successful new entrants gain ground.

In contrast, other views see more likely a scenario where integrated solutions are superior and thus high market concentration remains. Especially in the mid-term, when challenges are manifold.

Scenario-specific impact analysis

Scenario I: Incumbent players driving 5G

This scenario assumes that incumbent MNOs and traditional vendors will shape the evolution of 5G in Europe based on current performance requirements in the short term. Therefore, the entry of new system suppliers will be comparatively low. Overall, incumbent MNOs orchestrate an incipient ecosystem of new component suppliers and the traditional vendors pick and select suppliers according to their needs.

MNOs' orchestration efforts are assumed to bring increased competition to traditional vendors, albeit slowly and mostly for niche markets. Relatedly, a threat to MNOs is that a moderate demand for new services and from B2B applications hinders the entrance of new vendors and therefore their expectations of increased choice of suppliers.

The security restrictions applied in the US and several European countries for high-risk vendors, put existing vendors in a more comfortable position in the western market but it makes it even harder to enter big markets like China, currently around 50% of the 5G market. However, the sustained orchestration efforts of MNOs to bring new vendors in which traditional vendors also adapt their strategies. On the one hand, (some) traditional vendors started to contribute to the O-RAN specifications, on the other hand, these vendors can also adjust prices to sustain their market shares. An oopportunity for incumbent vendors is to maintain their market share, having more margin, timewise, to innovate their solutions compared to potential entrants, while taking the lead and shaping the ecosystem of new suppliers thanks to their bargaining power. In the long run, a limited number of more competitive multi-vendor offers emerge.

A threat for new RAN vendors is the limited opportunities to scale up, as Open RAN is only adopted in market niches. The emergence of new vendors will by large focus on the increasingly relevant private-sector networks. These new networks provide in particular opportunities for new vendors, as there are no path dependencies as in the large European consumer markets. This constitutes a risk for both MNOs and traditional vendors, as revenue opportunities in the emerging markets may neither be seized by traditional vendors nor by MNOs.

On a global scale, a policy-driven push for Open RAN in specific world regions on the one hand, and strong competition from Chinese players in other regions means this overall development could pose a long-term threat for the European industry at large when both traditional and new European vendors are lagging behind.

Scenario II: Slow pace of 5G Roll-Out

In this scenario, the impact on market competition in Europe is very low. Open RAN efforts in technology development are not serving as a game-changer and it is assumed that neither efforts to increase supplier diversity, nor efforts to spur demand in verticals prove to be successful in the medium term. The scenario is the most pessimistic one, but several interviewees worried this is the scenario where certain European Member States are moving towards.

5G will not be fully deployed in the mid-term, under this scenario, particularly not in the private network market. Even though it represents a small part of the overall market, many potential new entrants on the supply and connectivity sides are focusing on B2B use cases, seeking to have a competitive edge by specialising to meet the specific requirements of each use case. In certain countries, demand from businesses is not yet mature; there, B2B use cases are still rather limited to big companies, and the choices of equipment to rollout will only be taken in the long term.

One driver of this scenario is also a lack of cash available to MNOs, especially in those countries in which the prices of the licenses auctioned skyrocketed. In certain countries, such as Belgium, B2C demand for 5G is low, and ARPU is estimated to remain flat.[61] In other countries, 5G rollouts are already happening, and it seems unrealistic that in the longer-term horizon of these scenarios 5G rollout will remain low. However, an evolution at different speeds in different countries represents a threat to Europe in itself, since the deployment of 5G-and, in turn, the use cases it enables-is expected to bring advantages in terms of economic competitiveness.

A key threat in this scenario in the long-term is that technological trends and market developments in other world regions are not being effectively considered by traditional vendors – which might underestimate the disruptive potential of the emerging software-based technologies. Even more pronounced than in Scenario 1, a low level of demand and limited competition in Europe also has severe consequences in terms of competitiveness between regions. Therefore, this scenario would also have a negative overall impact on Europe.

Scenario III: Open RAN as game-changer

In this scenario market competition increases considerably as standardisation efforts lead to promising results for modularisation of the market, covering the Open RAN splits and the quick pace of multi-vendor deployments. Demand by the vertical industry for new solutions is high and new opportunities for all vendors and MNOs emerge. All other concerns aside, for the EU ecosystem as a whole, higher innovation incentives would be an opportunity to help enable new use cases and services.

In the mid-term, traditional and new entrants compete increasingly in the creation of private networks, leading to a scaling-up of some new entrants. Due to viable use cases, SMEs can convince private investors to fund this scale-up.

While this scenario might lead to a situation in which strong incumbent players and new vendors remain competitive, several interviewees highlight the risk of a lack of a strong European vendor ecosystem and a need for policy to support such a development. Currently, foreign players are deemed to be better positioned to enter the market as either new modular vendors or system integrators. Several interviewees mentioned that new entrants with the highest potential are foreign companies. They were concerned that in Europe, an ecosystem is missing. This lack of an early ecosystem could cause Europe to miss on the opportunity for an emerging market. To be more specific, US-based companies dominate the 'software level', while Indian IT companies like Radisys can leverage on significant IT bases and engineering manpower and much lower ARPUs than in European markets, which puts extra pressure on MNOs to explore a change away from the systems of traditional vendors. Some respondents expect that competition impact is felt most in the software

61 BIPT (2020)

and application elements/layers of the supply chain because software requires less investment and is thus less of a hurdle to enter the market. Hence, the scenario could represent a threat for the European supply ecosystem in terms of the distribution of market shares, after a market shake-up induced by substantial new entry of foreign players.

However, cybersecurity concerns in Europe may limit the entry of new foreign players in this scenario. In addition, there may still be room in the market for traditional solutions, especially if the pre-integration of components remains more cost-efficient. Moreover, even if RAN deployments rely upon open interfaces, traditional vendors may still be the ones providing the different elements and maintaining high market shares. This is already a reality when looking at different domains in the entire network (e.g., partnering with Ericsson for the Core and with Nokia for the RAN). Still, this scenario will bring a higher choice for operators.

While the 5G supply markets are characterised by high levels of competition in the medium term in this scenario, the longer-term likelihood of this scenario was questioned by some respondents, which expect a market consolidation after a few years. According to this view, a very diverse ecosystem would not be a lasting one. Rather, a reverse trend towards consolidation would take over the market, albeit with a potential shake-up in terms of dominant players.

Scenario IV: Open RAN for Big Tech

As network functions and elements become increasingly virtual, Big Tech players may leverage their cloud and software capabilities to move into the connectivity and supply domains with innovative solutions. Moreover, their financial strength allows them to overtake existing players and new entrants (for instance, Microsoft has acquired Metaswitch and Affirmed Networks, which are companies doing software for the core network). GAFAM companies engaging in the RAN market could represent a threat to incumbent vendors, SMEs and operators.

Threats to incumbent vendors directly arise from a greater presence and dominance of GAFAM companies. Europe still maintains an advantage over the US in RAN equipment, but the increasing transition towards cloudification and software-defined networks pose a threat to EU vendors' current business models.

GAFAM may focus on the emerging private networks (i.e., the enterprise, B2B market) first, rather than on public networks (i.e., the mass market). A key threat for traditional vendors and MNOs is, that these markets and revenue opportunities are not being effectively addressed.

However, for GAFAM the core network might be more interesting than the RAN because the core network is easier centralised, and closer to their current skills and infrastructure, based on data centres. They may expand, for instance moving their DC footprint to the edge. They could leverage their cloud capability to host applications. They may thus enter the application side, offering capabilities on-premise that are hosted in their edge cloud, thus extending the reach of their cloud services. This was likened to pushing core functionality close to the edge. Recent news has reported deals (e.g., starring Nokia or Telenet) in which Google is the responsible party to move software intelligence to the cloud, to run certain virtual functions in their DC. But this is more related to the core than the RAN.

To which extent GAFAM are able and willing to enter the RAN equipment market is uncertain, since it requires different capabilities to their current ones, as well as a more specific type of software. Some argue there is a realistic threat to bring RAN equipment and functions to their clouds, and that Open RAN stimulates this move to the cloud and Big Tech (e.g. TIP project is lead by Facebook). Others believe this is mistaken. The latter offers the following reasoning: The trend towards radio access network centralisation is unrelated to the opening of interfaces. This centralisation/cloudification of the radio is already a technical possibility. In fact, in March 2021, Nokia announced that it would put its radio in Microsoft, Google and Amazon's clouds. However, this would not have a significant impact on competition, since only a small part of the processing of a base station can be centralised. Most of the processing must still happen on-site since otherwise, latencies would increase beyond the amounts to tolerate. And RAN hardware needs to remain on-site, as it cannot be centralised. However, GAFAMs do not have the capabilities to deal with this specific on-site hardware. While they could invest to learn about it, the benefit of doing so is questioned, so it seems implausible according to these interviewees. The companies with specialised expertise to address this hardware are Qualcomm, Intel, Marvel, etc. But they do not do cloud nor have the ambition to operate a network. Rather they are specialised in providing the chipsets that perform the processing.

When looking at the entire network, this scenario would represent a threat for MNOs if they just move from a concentrated equipment market of vendors to an oligopoly in the cloud. In addition, this scenario brings threats to MNOs regarding competition on the demand side. As added value will shift from connectivity itself to the cloud, the future value generation of MNOs is at risk to decline. Another realistic threat is that Big Tech players dominate the end-user services layer by offering more value-added OTT services, and MNOs remain stuck offering the least profitable part of the chain, i.e., becoming “dumb pipes”. Additionally, they may enter the connectivity provision market and increase competition.

In the mid to long-term, GAFAMs may enter the connectivity space. Especially regarding the IoT market, they may have a competitive advantage from being better at software and IT integration. Today, traditional MNOs struggle to cover the needs of industrial customers, because they focus on selling capacity. However, this competition impact may be limited to B2B markets. The business case for becoming operators in public networks is unclear because it entails building new capabilities. More specifically, besides acquiring spectrum licenses, it entails managing regulations in each different country, doing local management of networks, dealing with thousands of base stations, etc.

c. Costs

Current situation and sources of impact

The main motivation for incumbent MNOs to be interested in an increasing supplier diversity are potential cost savings compared to the status quo. As published in the Baseline Report, the radio is the biggest cost component for MNOs when deploying network infrastructure, although a substantial amount of RAN CAPEX is not related to active equipment. In the long term, MNOs and potential supplier entrants expect Open RAN to become substantially more economical than closed approaches. However, traditional vendors dispute these claims.

It is generally understood that a direct outcome from increased competition in the RAN, ceteris paribus, would lower unit prices of equipment. More specifically, these CAPEX cost reductions would come from competition on prices, higher bargaining power from MNOs (as customers) and innovation. However, we need to look at the total cost of ownership (TCO) of Open RAN approaches versus traditional architectures. In this regard, OPEX and integration costs are seen as more determining components than CAPEX. The outcome from our interviews with relevant experts shows that there is contention regarding the potential of Open RAN to yield OPEX savings: the main points of contention between incumbent supply- and demand-side stakeholders relate to operational performance (mainly energy efficiency), system integration efforts, and the cost-efficiency of network upgrades. In addition, the lack of availability of transparent, up-to-date figures makes it difficult to provide quantitative estimations of the impact of Open RAN on TCO.

Notwithstanding the limited data and uncertainty, this section discusses a series of compelling and logical arguments regarding the impact of Open RAN in general and for the different scenarios described above.

Current situation and downsides in the short term

CAPEX costs of purchasing equipment are expected to drop due to competition and the resulting innovation. Higher interoperability of vendors and network equipment across RAN elements, a broadening landscape of providers, higher flexibility and bargaining power for operators, who will have the ability to choose the best and cheapest technologies in a “pick and mix” style; all these aspects will lead to a reduction in CAPEX in those scenarios where it is assumed that mature standards are a reality and Open RAN is assumed to be pervasively adopted.

However, it is important to look at the costs from a timing perspective. While standardising internal RAN interfaces may lead to more competition, the main question behind the adoption of Open RAN architectures will be the affordability of multi-vendor systems compared to integrated solutions:

- Both MNOs and vendors agree that in the short term, Open RAN will not be more economical nor better performant than the current integrated solutions from traditional vendors. Rather, implementing Open RAN would be more expensive with the current level of maturity and even during the first years after that.
- Respondents expect Open RAN not to be mature enough to be deployed widely until 3-4 years from today. And at first, Open RAN deployments will not deliver the same efficiency as traditional solutions in terms of features and power consumption. MNOs’ expectations for Open RAN to achieve parity and start outperforming traditional solutions in Europe place this break-even event at 5 to 10 years from now.

The main reasons why Open RAN will be less financially feasible than traditional approaches in the short to medium term are the following:

- The scale of small suppliers: As the ecosystem evolves and reaches a greater scale, the cost-efficiency of smaller suppliers is also expected to improve due to learning and economies of scale.
- Worse performance in terms of power consumption compared to traditional solutions: Traditional vendors design chips that are application-specific, and thus are optimised to manage layer 1 of the RAN, which is responsible for roughly 80% of the power consumption. This software- and hardware-based optimisation is done on the chipset. In contrast, the chips that are used to manage the RAN are general-purpose processors, meaning they are not optimised to manage this layer 1 of the RAN. While general-purpose computing can reduce costs, performance is still a big challenge, and it currently cannot compete with dedicated chipsets for RAN in terms of energy efficiency. Open RAN proponents expect that, in the future, a system based on these chipsets will be at parity with traditional RAN solutions in terms of power consumption. Other experts argue that, even in the long term, tailor-made hardware will be more optimised than general-purpose one, in terms of performance and energy efficiency.
- A technical challenge for multi-vendor solutions: Scaling up to support complex feature sets (such as those of big MNOs) in dense urban environments poses technical challenges that are not easy to be overcome.
- Integration and lifecycle management: There are extra integration costs of a multi-vendor environment, which also pose a concern in the longer term (see section 3.3); However, integration costs would be an even bigger challenge at the beginning, with a lower scale of Open RAN deployments

Long-term cost impact analysis: OPEX

A considerable amount of the expenses from base stations are operational (OPEX) in nature, including the rental of the sites, maintenance, energy consumption of these cell sites, etc. The debate of potential OPEX savings revolves around the performance of Open RAN versus traditional solutions. Here, by the performance, we refer to the energy consumed to generate a certain power output for a given level of coverage.

Most of the potential impact of Open RAN on costs would come from having software and hardware that is more efficient in terms of energy consumption. Enhanced performance would mean that you need less size and weight, and thus less steel, to achieve the same coverage. In turn, this would also lower rent costs since, in urban areas, these costs arise partly from the need to convince the site/building owners of allowing the installation of sizeable pieces of hardware. However, this potential for cost savings is far from clear. In the long run, MNOs and potential entrant suppliers expect OPEX to be the main source of TCO savings. In contrast, other experts argue that the current cost-efficiency of traditional vendors' solutions (based on special-purpose equipment and designed for optimisation rather than interoperability) will keep innovating and remain more financially viable when considering the aggregate costs of deployments, especially for those with stringent QoS requirements.

Open RAN proponents expect that cheaper chipsets from entrant suppliers that specialise in general-purpose chip design will catch up with traditional RAN solutions in terms of energy efficiency. The following arguments are being brought forward:

- First, they argue that the specialised capabilities of dedicated chipset manufacturers are superior to those of incumbent RAN vendors when it comes to designing efficient chipsets. They expect such base station chips to be more optimised in this regard by design. According to them, Open RAN will help attract these types of players to build specific elements for telecom markets. MNOs and potential entrants see an interesting business case for these companies in entering the market of chipsets for base stations. Currently, they already supply chipsets for small cells.
- Second, the indirect increase in competition through Open RAN could spur innovation. New technologies will emerge, and disaggregation will allow MNOs to quickly adopt the most advanced discrete components.
- Third, related to the previous two points, potential new entrants are working on semi-specific chipsets, which will accelerate innovation. Chipset manufacturers, the most important players being Intel, Nvidia, Marvel, Qualcomm, Broadcomm, etc. are all investing in this new chipset design. For instance, Qualcomm announced recently that it will provide systems-on-a-chip to do massive MIMO on a chip a year from now.[62]
- Fourth, optimisation on the software layers could take advantage of these new chipset capabilities.
- Lastly, the expectation is that in the future these chipsets can be better because of economies of scale.

On the other hand, traditional vendors argue that Open RAN, multi-vendor approaches will likely still be less energy efficient compared to their own. They admit the possibility of innovation yielding more cost-efficient Open RAN solutions in the future, but highlight that it entails a considerable challenge with a highly uncertain future outcome. Furthermore, as the discussion in the energy efficiency dimension (Section 3.8) highlights, these innovations may not remain exclusive to Open RAN solutions and could be similarly employed in traditional proprietary RAN solutions. They argue that with the current level of maturity, the RU/DU split entails a trade-off: by increasing the number of suppliers, you can decrease the unit cost price of equipment, but to achieve the same performance of integrated RAN products, you would need to build more sites. And building additional cell sites involves duplicating those costs that are not related to active equipment, which represent over two-thirds of the total CAPEX of a site, as well as more energy consumption at the aggregate level. Therefore, they argue that the added value of an integrated solution consists of a more expensive radio (thus higher unit CAPEX) but at the benefit of needing fewer sites (and thus lower aggregate CAPEX and OPEX).

62 https://www.fiercewireless.com/tech/vodafone-qualcomm-team-up-for-open-ran-design

At present, there are no robust longitudinal comparable datasets on the costs of Open RAN solutions and traditional proprietary RAN solutions. The current analyses mainly compare Open RAN solutions which are in developmental stages and primarily deployed in low-density greenfield locations with mature proprietary RAN solutions often deployed in a variety of low-to-high density brownfield locations. The available datasets are therefore insufficiently conclusive to offer a definitive assessment on whether Open RAN will prevail over the proprietary RAN solutions in the long-term or vice-a-versa when the cost/benefit dichotomy is considered.

Long-term cost impact analysis: CAPEX

From an MNO's perspective, Open RAN is an opportunity to reduce capital expenditures (CAPEX). The acquisition cost of equipment is a component where higher competition between vendors can bring savings for MNOs. All else equal, competition at a more granular level of the supply chain will enlarge the ecosystem of viable supplier options, and in turn increase both the bargaining power of MNOs, thereby incentivising product innovation at the supply side. Altogether, this will decrease the prices of RAN elements.

More specifically, Radio Units are expected to become more commoditised in terms of their design due to the opening of interfaces (assuming standardisation efforts are successful). In addition, CAPEX costs will lower via the use of cheaper general-purpose chips.

MNOs expect the indirect effects of innovation to be more beneficial in the long run than the direct impact of higher competition on prices. The impact of innovation —due to disruption from the competition— on the costs of telecommunications equipment has been demonstrated in the past, when Huawei entered the market with no existing market share but a huge budget dedicated to R&D. This lowered TCOs in a cycle of about 5-6 years until a new status quo in terms of market structure was achieved at the point where more R&D investment would not yield substantial market share gains.

While a change in commercial conditions can disrupt the market, this kind of disruption would only have a short-term effect. In contrast, according to some of the interviewed experts, a disruption from a more efficient R&D structure, which would result in product innovation - yielding, for instance, the higher performance of base stations discussed in the OPEX section -, would have a quicker and lasting effect on TCO.

Integration costs

From an MNO's perspective, building networks from a more diverse ecosystem of suppliers will increase integration costs. Therefore, another issue to solve before RAN demonstrates its financial viability is the integration of discrete products from different vendors. So far, we have deliberately left this aspect aside. But in addition to the aspects discussed above, there are integration costs from mixing and matching products from multiple vendors, which is a cost that currently falls on the traditional vendor, as it sells an integrated, black box solution.

Disaggregation increases complexity on the demand side. With more vendors providing equipment for the same network, seamless integration of system components will be much more technically challenging, and therefore it will entail higher costs. O&M (operation and management) will be more complicated and costly in a multi-vendor environment. O&M expenses include security testing, life cycle product management of spare parts, new releases in one of the subcomponents, etc.

Today everything is provided by the vendor in an integrated fashion. However, traditional vendors will not take the responsibility to solve the issue for the entire (end-to-end) chain unless there is a business case for them. To do this integration in-house, MNOs would need to build the relevant capabilities, which would entail duplication costs unless new business models are adopted (for an in-depth discussion of system integrator models, see the section on the 'business models' impact dimension). Building such integration capabilities entails, among others, costs of training staff to acquire the required knowledge.

Once again, this impact dimension is the source of opposed views. On the one hand, traditional vendors argue that integration costs due to disaggregation will be a bottleneck to the financial outperformance of Open RAN over integrated solutions. This belief is generally shared for the short term, with the current level of maturity of Open RAN. On the other hand, incumbent MNOs and potential entrants believe the industry will adapt because of several reasons. One way to overcome this disaggregation is automation, which allows cost-efficiently dealing with the complexity of putting together multi-vendor architectures. Another way is by finding new business models for those MNOs that cannot do this integration in-house. Whether system integration costs overwhelm the promised savings of Open RAN will then depend on how much third-party integrators charge for it.

Boundaries of TCO savings from Open RAN and impact estimates

There is high uncertainty about the measurable, quantitative impact of Open RAN on TCO. Settling the debate will only be possible with reliable data. Currently, there is a lack of transparency regarding cost-savings expectations, and published forecasts based on tests are subject to strong disbelief by traditional vendors. Moreover, the experts we interviewed were not able to provide specific estimations, including those MNOs that are leading proponents of Open RAN. Therefore, this topic remains to be explored once-reliable studies become available. Nevertheless, we summarise the discussion on the question of quantitative estimates, which at least shows the expectations of different stakeholders in this regard.

- Traditional vendors dispute the figures reported in the Baseline Report, which were based on reports from network operators (Rakuten, China Mobile and T-Mobile). Such estimations claimed network TCO savings of up to 44% because of virtual and Open RAN and automation, compared to traditional RAN architectures. More specifically, OPEX and CAPEX savings estimations ranged from 40 to 53% and from 30 to 50%, respectively. This impact is also ambiguous in the sense that it relates to multiple technological and market trends. The next section will provide a discussion of parallel supply market trends that also promise to impact the TCO of network deployment and operation.
- While unable to confirm if these estimations are realistic, MNOs and chipset manufacturers argue that the potential for savings is clear. They argue the following: first, while Open RAN will not be more efficient than current integrated solutions from day one, it will also not be substantially worse. Second, in the long run, they claim that multi-vendor, open architectures to consume less energy than current systems, with expectations ranging from modest to drastic, even beyond the reported figures above. As mentioned before, the main argument was that many potential providers are already working on their novel products. Further, two respondents claimed that the white-label massive MIMO chips will be more energy-efficient than current market products from the start.
- In addition, a couple of MNOs mentioned that in a few months they would have enough base stations rolled out to provide comparative performance estimates with equipment from different vendors. However, MNOs admitted that they cannot provide reliable cost estimations at the moment. It is too early to tell; Open RAN is not mature yet.
- Regarding system integration costs and life cycle management, a quantitative estimate was also deemed as too difficult to provide at this stage.
- Finally, other stakeholders mentioned that it is hard for them to have a concrete understanding of the specific impact of Open RAN on costs, as they do not have access to the cost structures neither leading operators nor vendors.

These opinions show a marked distinction by stakeholder type; once again, the lack of available data complicates any fact-checking and the identification of underlying bias.

To lessen the limitation of the lack of availability of factual data, and to help give context and a quantitative reference, we gather and summarize estimates from independent, evidence-based sources. The main limitation remains since data from existing publications is independent of the scenarios described. The following paragraphs address CAPEX and OPEX, in this order. CAPEX is incurred when new sites are built, existing sites upgraded, or equipment replaced. In terms of CAPEX, the main potential impact of opening interfaces comes from competition pushing prices of RAN equipment down. In terms of OPEX, a main aspect of contention is whether open architectures will be more costly to provide the same performance or, on the contrary, the entry of new players will make base stations more energy efficient.

As presented in the Baseline Report of the present study, the global 4G and 5G infrastructure market is estimated to be valued at USD 56 bn. In the report, it is shown that roughly 35% of the market's value is related to the services, maintenance, installation costs, set-up fees and commercial-off-the-shelf hardware associated with establishing and operating a mobile network. The remaining two-thirds of capital expenses are related to infrastructure elements, including all network domains. In the European (EU-27) market, 60% of these expenses (about 2.8bn USD in total) are associated with the RAN domain. In comparison, 19% come from the core, 7% from transport and DCs, and 14% from operational support systems. One limitation recognized in the report is the inclusion of public networks only since the difficulty to differentiate between deployment types would lead to an inevitable overlap. Nevertheless, public networks account for the vast majority.

RAN equipment includes the radio (antennas), the baseband units or BBUs (which are split between the CU and DU), transmission equipment, etc. This equipment is installed on top of base station sites (i.e., towers and rooftops). A substantial part of capital expenses (CAPEX) from rolling out networks is not related to active telecom equipment, but to the acquisition of other assets such as spectrum licenses, civil works (cabinets, fences, antenna masts, etc.), long stretches of fibre backhaul to reach the site, and so on. Other CAPEX are related to setting up the sites, which includes, among others, labour costs. Operating the sites also involves recurrent expenses, which involves having contracts for rent, power, air conditioning, etc.

While deploying radio access equipment is only a small part of the overall cost structure of MNOs, it still involves sizeable amounts. A straightforward reason is the number of sites needed to provide national coverage with wireless networks. In total, according to TowerXchange research, there are around 600 thousand towers in Europe. The largest European MNOs deal with dozens of thousands of sites each. These are either directly owned, partly owned via joint ventures or associate entities, or leased from third-party infrastructure owners. There is a steady trend in the market to divest sites to neutral host network infrastructure owners such as Cellnex. For instance, according to its corporate website, Cellnex counts over a hundred thousand sites within its European portfolio (including ongoing transactions and planned rollouts). The resulting cost structure between capital and operating expenses will therefore also depend on the site ownership model adopted by MNOs.

For reference, we review the CAPEX per 5G site as estimated in other recent studies. Some studies model macrocell and small cell antenna sites, but for simplicity and clarity of comparison, we focus on macrocell costs only. In addition, these estimates do not include spectrum costs. Many assumptions are included to arrive at the reported estimations, for instance in terms of cost breakdowns per category, deployment area (e.g., brownfield vs. greenfield, urban vs. along highways), deployment model, etc. Therefore, we summarize the findings of the different studies separately.

First, the baseline scenario of the cost model in Oughton & Frias (2018) provides the following estimations for a non-virtualized 5G infrastructure, referring to the CAPEX of brownfield macrocell upgrades:1) 40,900 GBP for deploying a multicarrier base station; 2) 18,000 GBP for civil works, and 3) 20,000 GBP of fibre backhaul per km.

Second, we show the findings from the 5G NORMA project (2017). Again, it refers to their baseline scenario, for macrocell antenna sites. RF front end is the main driver of CAPEX, followed by civil works and acquisition costs. The other cost elements are 'antennas/feeder', bare metal baseband (BBU), transport and labour:

- They estimate 46,200 GBP in civil works and acquisition costs for a rooftop site in central London.
- Site costs are also influenced by the number of antennas. In this regard, massive MIMO technology also modulates costs. They assume that the cost of arrays with higher numbers of antennas (e.g., 32 or 64) in the same base station does not proportionally increase with the number of antennas. For example, a set up of 32 antennas is estimated to cost 4,800 GBP, while one with 64, 7,200 GBP.
- Baseband unit costs also fluctuate depending on the characteristics of the equipment assumed to be deployed. For a D-RAN deployment, where the baseband processing is performed at the antenna site, costs depend on the number of 2x2 MIMO streams and spatial beams that need to be processed. The estimated CAPEX cost of the BBUs is 3,750 GBP for a macrocell of a 20MHz 2x2 MIMO channel.

In their model, the authors differentiate between a D-RAN and a C-RAN architecture. The CAPEX of the earlier option is 18% lower than that of the latter. In addition, over their modelled period of eleven years, CAPEX amounts to around 25% of TCO. This is in line with insights we received from interviewed MNOs, which claimed that while the CAPEX of equipment is relevant, it is a relatively small percentage of TCO.

Third, a recent report by Barclays (2021) estimated the rollout costs that the German operator Drillisch would need to incur. The resulting per site CAPEX, including backhaul, is the following: 70,000€, for existing towers, and 170,000€ for newly built sites.

Greenfield deployments are more expensive than network upgrades. However, it is also simpler to deploy, which increases the speed of rollouts and the associated costs. Deploying an Open RAN architecture on top of legacy networks is a more challenging exercise, as it needs to consider the backward compatibility with already installed equipment.

They also note that site costs depend on the deployment model. If instead of rolling out its own sites, Drillisch would become a tenant of a third-party infrastructure owner, they estimate that the operator would pay an annual amount of 15,000€ per site for the lease.

Finally, the 5G PPP Automotive WG (2019) also estimate the costs of deploying a 5G site, in the context of connected driving use cases. In their baseline scenario, the estimated CAPEX are the following: 1) Site infrastructure (gNBs, network equipment, cabinets): 64,000€ per site, 2) Civil works: 20,500€ per site, 3) Fibre backhaul: 23,000€ per km.

Next, we consider the boundaries in terms of impact on operational expenses. As discussed before, the potential of Open RAN to reduce MNO OPEX mainly depends on the capacity of equipment from entrant suppliers to be more energy efficient. This performance requirement is highly linked to the performance of processors. Power consumption is an important source of OPEX for MNOs. The aforementioned large amount of RAN sites means that small savings per site would, all else equal, already be an incentive for MNOs to adopt Open RAN.

According to its latest annual report, Telefonica’s total annual energy consumption has been almost 7,000 GWh (Gigawatt hours) over the past few years. Broken down by type of network element, 44% of this amount came from cell sites and 35% from fixed switch sites.

Vodafone’s energy usage, also according to its 2020 Annual Report, was 3,810 GWh. It is unclear whether this consumption comes from only the operator’s sites that equipped with smart meters, or it includes the entire portfolio of directly and indirectly owned sites. Depending on this, the resulting energy consumption per base station would be between 63.5 and 30.5 MWh.

Once again, not everything is subject to be impacted by an opening of RAN interfaces. For instance, as explained in the section of this report covering the ‘Energy efficiency’ dimension, about a quarter of total power consumption at base stations comes from cooling systems, although this consumption depends on the type of cooling system and RAN architecture used.

The assessment in 5G NORMA provides a breakdown of macrocell antenna site operating expenses. Site rental is the largest cost driver, followed by energy consumption. Other OPEX are transport, maintenance and RAN equipment licensing costs. In their baseline scenario, they estimate a yearly OPEX of 10,000 GBP for power consumption, per site. However, they note that about 75% of this cost stems from business rates (a tax applied in the UK to non-residential properties). This tax aside, the estimated OPEX from energy consumption would be 2,500 GBP.

Parallel 5G supply market trends

Besides the opening of interfaces, parallel supply market trends also promise to have an impact on network TCO. More specifically, we mainly focus on the use of artificial intelligence to manage network functions (automation) and the disaggregation of network functions between hardware and software (virtualization). To the extent that these software network functions are brought to the cloud, this trend is related to cloudification. The impact of these trends is expected to be less uncertain and more straightforward than that of Open RAN: virtualization and artificial intelligence are current market trends that will bring OPEX down by optimising the efficiency of wireless networks.

Virtual RAN (vRAN) technology involves replacing hardware with software, which can result in significant cost savings in the overall deployment and managing of radio access networks. A more software-based network allows to create new instances or make modifications in a more agile way, compared to the status quo. For instance, it can avoid sending personnel to a location to make certain changes to the equipment. In addition, it can ease the barriers of entry for companies that specialize in the cloud stack and in providing software solutions. Entering the radio unit market requires much higher investments than providing software components and functionalities. In turn, large investments entail that developing cost-competitive products relies more on a large scale of operations and integrated entire system solutions. These required investments and scale represent a barrier to break into the market for smaller players, who are at a disadvantage compared to traditional vendors. Therefore, vRAN makes it less costly to provide discrete functionalities on top of an incumbent vendor's cloud RAN for niche segments, even if the RU/DU split is not open and interoperable in terms of equipment. Lastly, it must be noted that Open RAN is often based on vRAN, but it must not necessarily be the case. Open RAN can work on both bare-metal and vRAN. However, some interviewees believe it is not entirely independent in terms of market adoption, arguing that the competition impact of Open RAN will help stimulate the development of vRAN.

As discussed in scenario 4, cloudification is expected to exert its main impact at the core domain of the network. Cloud RAN is not expected to have a large impact in terms of costs or competition; processing can be entirely kept on the RAN site or be partly centralized on a data centre, either with a traditional or new vendor. However, most of this processing must remain ‘on site’.

Automation is one of the main cost benefits for virtualised networks, as it will further optimise network functions. Increasing degrees of automation are expected to decrease OPEX of network operation significantly. For instance, OPEX will lower due to cheaper maintenance, since algorithmic approaches can automatically identify and fix problems in software configurations. It was noted that to leverage automation to the fullest, future networks need to include it from design (contrary to on top like today).

Scenario-specific impact analysis

Most interviewees noted their belief that the drafted scenarios are not mutually exclusive. Rather, reality would probably result in a hybrid scenario that combines several of the assumed trends. While this is a general perception, it is especially relevant for this dimension, where uncertainty prevented our interviewees from making quantifiable estimations regarding the impact on costs. Therefore, it is also difficult to make clear distinctions about the impact of this dimension on a scenario by scenario basis.

Scenario I: Incumbent players driving 5G

In this scenario, incumbent vendors and MNOs drive the introduction of 5G. MNOs have found it financially feasible (or even beneficial) to invest in vRAN and Cloud RAN as intermediate solutions and gradually introduce deploying Open RAN (even if proprietary) in the long run. Traditional vendors anticipate these developments and adjust their prices at least to some extent. As a result, total operating costs at least slightly decrease for MNOs.

Intensive R&I and testing of the pros and cons of an open ecosystem provides MNOs with an opportunity to decrease the dependency on single suppliers at least in the long run. By doing so, it can help keep the challenging costs of system integration in check when compared to a scenario where a dominant system integrator appears. However, the required funds to invest in R&D may only be available to a select group of incumbent operators. The ability of MNOs to afford new Open RAN deployments is questioned. As new deployments are lacking scale, OPEX for new solutions may remain comparatively high compared with current solutions.

Scenario II: Slow pace of 5G roll-out

Scenario 2 would resemble the status quo the most, in terms of costs. This stems from the assumptions of a slow rollout of Open RAN-based 5G networks and the low entry of new players. These assumptions would entail the following effects regarding the main cost components identified before:

- First, a lack of multi-vendor RAN deployments would mean a lack of need for system integration efforts, which are the main source of additional costs compared to the status quo.
- Second, the bargaining power of vendors would remain largely unchanged, as well as their business models. Therefore, the main drivers of lower equipment costs would not be realised.
- Third, innovation incentives would not increase. Two other assumptions of this scenario, namely a low level of EU cohesion and a low level of policy support for increasing standards and diversity would reinforce this. Innovation incentives are the main driver to decrease operating expenses via performance improvements regarding power consumption.

A realistic driver of Scenario 2 was deemed to be a lack of cash by European MNOs. After spectrum auctions, their current availability of funds and operating margins are lower than at the start of the previous generations. Therefore, they do not have as much capacity to invest, which represents a current cost bottleneck for the deployment of new networks. While this could lead to a push for more vendor diversity, it could also contribute to an overall slower uptake of 5G in Europe. In addition, from the perspective of MNOs, the diverse implementation of the cybersecurity toolbox in the EU Member States, may even further limit the supplier base and cause even higher investments for system replacement in the future.

Scenario III: Open RAN as game-changer

The advancement of fully virtualized networks and high consumer and business demand for innovative 5G solutions incentivize a fast 5G development pathway. While OPEX of Open RAN deployments catches up due to economies of scale, traditional vendors may react by stronger in-house innovation and cost reductions, while successfully maintaining their all-in-one business models. The pace of innovation is high, and so is the scale of deployments. Due to strong competition in the market, deployment costs overall decrease.

This scenario would drive equipment costs down the most, because of the competitive pressures on traditional vendors. OPEX could go down from the fact that external innovation is incorporated into the products of traditional vendors. However, the overall TCO remains unclear due to the uncertainty about the effect of multi-vendor solutions regarding performance and OPEX, even though this scenario would bring the biggest opportunity for multi-vendor solutions to catch up with integrated ones in the long run.

Integration costs would first be negatively impacted by the need to manage contracts and assure timely maintenance in a context with multiple RAN providers. However, as new vendors and traditional vendors are in strong competition, integration costs may level out in the medium term. Following a phase of strong competition on costs by vendors, a similar evolution towards concentration could happen in the medium to long term under this scenario.

However, a threat of this scenario is that the level of increased complexity is vastly underestimated. Some interviewees argued that software is where most problems come from (e.g., network outages). A related threat of multi-vendor, disaggregated architectures is the potential lack of a single entity that is responsible for network failures. As a result, redundant security checks and troubleshooting can increase costs.

Finally, Open RAN will not have an impact overnight. Therefore, we need to take into account the time component of costs. This scenario assumes that progress in terms of technological and market readiness of Open RAN is being made fast. On the OPEX side, it means that it brings the highest potential for multi-vendor solutions to catch up with integrated ones. In practice, this may take some years to be realistic, even in scenarios where 5G rollouts and standardisation efforts advance at an optimistic pace. Furthermore, this scenario provides the optimal context for small players to find a business case and invest in R&D, and thus for innovation to advance until consolidation takes place.

Scenario IV: 5G for Big Tech

A scenario where the entry of GAFAM brings a disruption in terms of costs because of the opening of interfaces was argued to not be realistic. The threat of dominance by Big Tech is assumed largely due to their cloud capabilities. However, the centralisation/cloudification of the radio is but a technical option without a significant impact in terms of operating costs.

Radio access network centralisation and Open RAN (open interfaces) are different trends with different impacts. Open RAN can be done by keeping the processing on the site or partly centralising it on a data centre. And this centralised processing can be done with a traditional vendor as well.

According to the detailed description by one MNO, the centralisation of the radio would not imply an architecture that would bring a paradigm change. The only part of the processing of a base station that can be centralised is equivalent to about just 10% of the OPEX of that base station. Most of the processing must still happen on-site. Otherwise, latencies would increase beyond tolerable amounts. Moreover, the radio's hardware, being the antenna, the amplifier or the physical layer, needs to remain at the base station, on-site (it cannot be centralised). And the operation of sites by MNOs involves expenses for rent, power consumption, air conditioning, etc.

To achieve savings from centralising base station hardware and thus doing some aspects commonly across base stations, large amounts of dark optic fibre need to be installed to reach the site (more than now because that link would not be as efficient). But not all European MNOs have abundant dark fibre available, especially smaller ones. While in Japan, for instance, deploying dark fibre anywhere is affordable, this is not the case in Europe. This would make the business case of a centralised architecture (compared to a distributed one) negative in many cases.

Bringing this RAN processing to the cloud would have a low impact on performance as well, according to this view. Regarding performance, there is not much you can do with a centralised architecture that you cannot do with a decentralised one, even if it is done differently.

In conclusion, if tech companies enter the market to take the 10% of a base station’s processing, the impact on costs for MNOs would be negligible.

d. Business models and requirements

Current situation and sources of impact

The evolving 5G market also promises to exert an impact on the business models of current supply-side companies, as well as on demand-side ones. New architectures will place more relevance on certain roles, such as that of system integrators. System integrator models are subject to change, and entirely new models may emerge.

System integrator (SI)

The most relevant impact from the trend of the opening of interfaces in terms of novel business models in the supply market will revolve around the role of system integration. Uncertain extra costs of system integration can 'make or break' the business case for operators, especially smaller ones.[63] The SI role could be offered in different ways in the future. While the focus of SI is on MNOs, SIs can bring value to different types of customers: public networks, private network operators and neutral hosts as well.

Today, traditional vendors manage multi-vendor networks, which offer proprietary, integrated systems. However, they do not do that on a component level. With a more open architecture in the future, economic incentives for traditional vendors to focus on SI is potentially removed. Unless there is a business case, vendors will not take responsibility to solve issues for the entire end-to-end chain for lifecycle product management, security testing, fixing of errors. It is therefore uncertain who will play the integrator role: it could be either the operator (or customer) itself, a vendor, or a third party. With the hypothetical opening of RAN interfaces, integration becomes a challenge for MNOs as well as a business opportunity for third parties.

A key challenge in disaggregated RAN architectures is that the integrator may not be able to fix problems at every single point of the value chain, due to a lack of domain-specific knowledge. Therefore, the product provider may still need to be involved. The integrator may just focus on integrating components rather than on resolving issues. The challenge with Open RAN architectures is therefore the willingness of the SI to take the responsibility for the reliability of the entire network, in case of service downgrade or connectivity being unstable. The vacancy of this role brings the risk of networks being less reliable.

According to our interviewees, the integration at the cloud level, as well as for hardware and software components for different vendors is not a challenge on the technical level but integrating discrete radio functions is still a challenge today. The biggest challenge in a disaggregated system is reintegration and orchestration so the different elements work flawlessly and highly automated. Some respondents were confident that the industry will adapt, as this has been the case in other industries that dealt with increasing modularity. For Open RAN, the bet is that standardisation would facilitate interoperability. Virtualisation and the use of software solutions will make certain players more able to play this role.

The big MNOs in our interviewee sample are exploring the possibility of doing the integration alone but admitted that this is a challenging task. Another respondent shared its informed belief that only a few of the European MNOs probably have the R&D capabilities required to perform the SI role in-house, leaving the majority highly dependent on third parties.

With the expected increasing modularity of the supply market in the longer time horizon, MNOs would have the responsibility to solve the resulting integration challenge. To avoid duplication costs from each MNO doing the same integration effort for a given chosen set of suppliers, only novel business models would allow to share these costs. Therefore, four integration options exist:

63 See Taga et al. (2021) for market players that can play this SI role.

MNO in-house model: Integration would mean putting the discrete elements in a lab and figuring out how to make them work together, which entails new in-house costs regarding infrastructure, R&D, personnel, etc. The main drawback of this model is that it could entail duplicating all these costs, which would make it the least financially viable model. For larger MNOs, taking the integration responsibility themselves could make them less dependent on a potentially dominant supplier.

Outsourcing model: This would mean outsourcing the task to a third party, which could be a specialised SI. This will be more likely for smaller MNOs that do not have the resources to build the required know-how by themselves. The risk of this is escaping a traditional vendor lock in to get into a supplier lock in on this SI. Another potential drawback is that MNOs may not know who to address in case of a problem with a component unless the SI integrator provides an all-in-one service function.
In this model, some duplication of costs would occur, because each MNO (or private network operator) would have to buy a specific integration. However, duplication costs would not be as high as in the MNO in-house model due to economies of scale and lower unit costs. The lower transparency and higher dependence on this third-party would probably still keep the price higher than in a marketplace model.

Marketplace model: In this model, the industry would coordinate and share costs via a kind of marketplace where operators, vendors or specialised SIs can align their integration research. The basic premise is that the integration effort for a specific combination of vendors can be valuable for other operators and will reduce duplication efforts. This is not like a certified integration but a continuous research service for updating system elements. One challenge of this model is a high level of industry coordination needed to organise or allocate a budget and to make sure this model is being taken up. A third-party organization could facilitate this and play the platform coordination role. As a jointly funded and neutral entity, this could offer more price transparency and help to avoid duplication of efforts, being compatible with an EU wide security model.

Vendor-led model: Much like the current situation, vendors themselves, traditional or not, can play this role. As mentioned before, traditional vendors already have similar capabilities. In this case, a vendor could do the integration before selling the solution or sell this integration as an after-sales service. There is a similar offering in the market already, namely Rakuten's RCP (Rakuten Communications Platform): RCP is not only doing integration in-house but offering the complete blueprint of a private network, including the cloud and management platforms. If this model becomes the predominant one will limit the increased freedom of choice (theoretically) brought by Open RAN to some extent, as MNOs would likely rely on a limited number of proprietary solutions.

In addition, the variety of software modules composing the networks mean that there will be different levels of releases, and different capabilities in different networks being implemented. To guarantee EU wide security levels, a very strong process needs to be put in place to guarantee consistency of all implementation in the EU with the desired security levels. Certification will become a key aspect ex-ante – which may increase system integration costs.

Current vendor models vs new models

The emerging new vendor models, together with the parallel and mutually influenced trends of automation and increasing reliance on both (open-source) software and commercial-of-the-shelf (COTS) hardware, could bring an opportunity for new business models to emerge. However, open interfaces[64] do not directly imply the use of non-proprietary software/code and hardware, so hybrid models between a proprietary 'black box' and an open-source-based 'white-box' are still likely to co-

64 The term "open" in Open RAN refers to the subdivision of network blocks into subcomponents through the definition of new interfaces. However, these subcomponents can be built out using anything from open-source to proprietary technology.

exist with the end-to-end ones reviewed below. In addition, higher network modularity will likely increase the presence of subscription models.

Current vendor models are based on a closed approach, providing integrated, proprietary solutions and additional services for the entire life-cycle of the equipment, typically an entire generation. These additional services include software updates, intervention when there are issues to solve, replacement of parts, training, etc. Recently, MNOs have extended these deals to also subcontract the management of their networks to vendors, intending to increase flexibility and reduce costs.

Often the current vendor model is structured as a razor-blade type of revenue model, in which the equipment is priced very competitively and even financed by the vendor at more beneficial conditions than a financial institution. Spreading upfront CAPEX into recurrent cash outflows over several years increases the ability of those MNOs with liquidity constraints to commit to investments in network equipment. This is compensated by more lucrative services bound MNOs to specific vendors during the whole lifetime of the equipment. For those MNOs with limited liquidity, seeking (affordable) external financing when deploying multi-vendor networks from multiple, modular RAN elements may be a challenge as upfront investment costs will be higher.

The integrated vendor model offers a superior value proposition concerning system integration as it is more cost-efficient (done in-house by the vendor) and operators know what door to knock when there are performance problems. The downside is a higher degree of dependency of MNOs on vendors and the model creates a barrier to entry for smaller competitors. The price transparency for MNOs is lower and bargaining power for vendors accumulates if the number of available vendors is low. The resulting profitability from the vendor lock-in and induced market power is the main reason vendors prefer to offer the various RAN elements in the form of proprietary closed and integrated systems.

Subscription models: As it is already the case for cloud computing, the increasing relevance of software may cause a move toward subscription models. As a result, MNO cost structures can shift to become more dominated by operating expenses. From an MNO perspective, software-based solutions and cloud computing will lower the CAPEX of what is strictly equipment while recurring payments for licenses and virtual functions provided as-a-service will increase. This effect will be more significant for the core than the radio networks; as mentioned before, several RAN functions (such as a high percentage of the processing) need to remain on-site (i.e., in the physical location of a base station). In contrast, core functions are more subject to be impacted by ‘cloudification’.

Potential entrants expect to leverage the parallel technological trends of software. [65][66] RIC platforms offer life cycle management, hosting and dynamic orchestration of microservices across the RAN. Using an open approach, a RIC platform allows third-party developers to create their apps on top of APIs.

A key aspect enabled by Open RAN is that these software elements are compatible to operate on equipment and silicon platforms of multiple vendors, allowing system integrators, operators or private network owners to choose their preferred hardware and software at a more granular level than today.

‘White box’ model based on open-source: In contrast to a business model of discrete component provision as described above, a ‘white-box’ approach represents a novel type of end-to-end business model. This approach consists of building a multi-vendor solution by buying certain COTS hardware elements from a manufacturer (e.g., for the radio unit or servers, small cells, general-purpose processors, etc.), possibly complementing it with its own hardware elements and software based on open-source. These open architectures would leverage standardised Open RAN splits and the virtualisation of many RAN components.

65 See, for instance, the product portfolio in https://accelleran.com
66 See, for instance, https://www.ericsson.com/en/blog/2020/11/next-generation-cloud-ran-management-and-orchestration

This model may be adopted by traditional vendors or MNOs, but new entrants with system integrator capabilities are the most likely player to adopt it in the nearer term. For them, it is a way to offer a competitive value proposition vis-a-vis current vendor models. An end-to-end offer would, all else equal, yield to the supplier more visibility and a tighter relationship with the demand-side customer, and, therefore, a higher level of control over the supply chain. These white-box solutions can be supplied to MNOs, local network operators, private network owners or neutral hosts (i.e., infrastructure owners that host multiple tenant operators in their infrastructure).

Overall, white-box models could offer lower equipment costs compared to current vendor models, due to their use of commodity, COTS hardware and flexible, multi-vendor architectures. A further opportunity for MNOs from moving to white-box models based on open-source software is that they would reduce, all else equal, the amounts of licensing fees paid for network updates. For non-incumbent vendors, this model also entails a lower barrier to entry, since it relies on third-party solutions rather than on building internal R&D capabilities, even though it requires SI skills. Therefore, this model would drive supplier differentiation in the RAN domain. On the downside, the value proposition offered to customers would be inferior in terms of troubleshooting simplicity and continuous high investment costs for building up system integration capabilities, due to a lack of a single, clearly identified actor that claims responsibility for network failure or misperformance.

Demand-side: the case of private networks

More or less directly, Open RAN can also have an impact on the business models of the demand-side, that is, of connectivity service providers and network operators. Therefore, we also focus on the private networks for B2B - vertical market use cases.

Private networks are expected to become more relevant with 5G. The main reason is the forecasted emergence of challenging use cases, the stringent requirements of which can hardly be addressed by previous generation technologies. Each use case has its own very specific QoS requirements in terms of latency, reliability, data storage, the need for edge vs public cloud, etc. Meeting these requirements will rely, in large part, on virtual solutions, which will need to be continuously updated to meet the needs of innovative use cases. Addressing niche markets via private networks demand therefore requires different capabilities compared to addressing public ones. One expert voice noted that timely upgrading public networks to meet these specific requirements is too slow and not flexible enough.

Open RAN, disaggregation and private deployments are expected to enable networks to be more flexible, by incentivising use case-specific software developers and niche connectivity providers to emerge and scale. These trends mutually influence each other: lowering barriers to entry for different players can speed up the deployment of private networks, which in turn makes the opportunities to scale growth.

Private networks can be owned and operated by the site owners or by third parties. Several interviewees believe that self-deploying private networks are a realistic option only for (a) big companies with large manufacturing plants and (b) other sizable local deployments (e.g., a port or a hospital), the reason being that substantial knowledge and size are needed. Most companies would then rely on traditional operators or vendors to provide them with private networks. In such a case, these operators can be the same MNOs that operate public networks, neutral hosts or a local ‘micro operator’.

Neutral hosts are non-operator third parties that deploy and/or manage infrastructure. Neutral hosts own network infrastructure and aim to lease wholesale access to multiple M(V)NOs tenants, thereby spreading costs across operators and making deployment more feasible (GSMA, 2018). M(V)NOs could thus provide the connectivity service relying on neutral hosts.

A micro operator (µO) is a connectivity service provider that does not own spectrum and only operates within a specific site or area, having a local monopoly within the space it serves from exclusive access to site-specific content or infrastructure.[67]

Lastly, private networks may have their own spectrum. Consequently, spectrum allocation models will also play a role, especially regarding the dichotomy to reserve certain bands for industrial use cases and local deployments or for public MNO networks.

In Germany, industrial players lobbied for spectrum to be allocated directly to them, based on the argument that the services of public network MNOs had failed to cover their specific needs for years. The country's regulators reportedly allocated private spectrum licenses directly to the industry, more specifically to large companies with big production plants such as Bosch, BMW, Siemens and Volkswagen. This allocation of spectrum directly to industry players remains a controversial issue, and several interviewees raised the concern that fragmenting the spectrum inflates auction prices since it makes the remaining spectrum available to MNOs even more scarce. In consequence, it lowers the budget available to them to invest in networks. It may also lower competition between MNOs if the spectrum fragmentation reduces the number of licenses or the size of the blocks auctioned. However, this may be mitigated by making more spectrum available at the same time, even if this is done in a kind of flexible, layered approach (as in the case of CBRS in the US), where some repurposed spectrum is still reserved in case of an emergency.

Scenario-specific assessment

Scenario I: Incumbent players driving 5G

This scenario assumes a future where incumbent MNOs and traditional vendors orchestrate the 5G ecosystem. New suppliers are only being integrated gradually, in the medium, to long term.

In this scenario, business models and system integration for the supply chain are likely to remain by large unchanged, as it seems unlikely that, as of today, European MNOs can test and integrate multiple vendors elements themselves. Building these capabilities is very expensive, requiring huge manpower and R&D investments. The belief in our sample of respondents was that aside —maybe— the one or two biggest incumbents, the rest would struggle to have the required budget. While MNOs have the knowledge and expertise to lead system integration R&D efforts, a vast majority of them do not have the funds. Recent anecdotal evidence supports this conclusion:

- First, the recent MoU signed by the four biggest European MNOs (DTAG, Orange, Vodafone and Telefónica) establishes a commitment to seek public funding to support, among others, R&D activities and test labs.
- Second, many MNOs have outsourced the managing of their network to vendors (including day-to-day management, software updates, etc.), which is seen to be motivated by budget constraints.
- Third, with recent 5G rollout announcements, MNOs have chosen to rely on traditional vendors.

Nevertheless, some large MNOs feel confident that they have the knowledge expertise to potentially adopt an in-house model in the future, which might put some pressure on incumbent vendors. Some MNOs are even exploring white-box models, in which they assemble their solution, with a mix of in-house and third-party elements. These white-boxes rely on a modular supply and open-source software. For instance, AT&T has reportedly been working on Linux-based software.

Even in a scenario where MNOs orchestrate the emerging 5G ecosystem, their current connectivity service business models face challenges. In Europe, the benefits of 5G are not likely to be perceived

67 See Ahokangas et al. (2016)

by consumers as ground-breaking, and their willingness to pay extra is therefore limited. As shown in the Baseline Report from Task 1[68], average revenues per user in Europe are stagnant and substantially lower than in North America. To increase demand on the consumer side, MNOs may need to come up with innovative products in the realm of gaming, augmented and virtual reality. For instance, via B2B2C approaches where a partner develops a console that is enabled with VR and works on 5G, incorporating a subscription. Therefore, a threat for Europe is that MNOs or other players are not able to come up with innovative business models that make new B2C or B2B use cases attractive for end-users and enterprises, respectively.

The customers will opt for the network with the best performance. It is predicted that the churn rate will be increasingly driven by network performance. If MNOs will face performance problems due to the implementation of not yet mature O-RAN specifications, they will face losses due to increased churns to MNOs running 5G 3GPP solutions.

The scenario offers an opportunity for incumbent vendors to ensure new entrants' solutions are pre-integrated into their proprietary Open RAN solutions. The limited scale of Open RAN deployments, together with the dominant position of incumbent players, would make suppliers less able to access external capital and remain reliant on the decisions of new vendors to include them into their products, therefore maintaining their barrier to entry. In addition, the assumptions of this scenario would likely make the value proposition of the integrated model a compelling one for MNOs, thanks to retaining the responsibility of troubleshooting and fixing problems. Altogether, it would offer no incentive for incumbent vendors to adopt new business models even if they adopt Open RAN. Rather, they would try to maintain the competitive advantage of pre-integrated solutions.

A key risk of this scenario is that demand by the vertical business sector is not being matched by existing supply. Large companies may want to customise their private networks (for example at the software layer, but maybe also at the hardware equipment layer) to meet their specific QoS requirements. Because Open RAN is seen as a driver for differentiation and innovative solutions, according to this view there would be opportunities for new entrants to enter the vendor market (see the impact on market competition). But the need for differentiation is also felt on the connectivity side, incentivising the entry of new players at the demand side as well. Currently, the B2B connectivity market remains concentrated among big MNOs, but it offers opportunities for smaller (virtual) operators or OTT services providers. Examples of MVNOs include Cubic Telecom and Transatel for automotive use cases.

Scenario II: Slow pace of 5G Roll-Out

In this scenario closed approaches will be dominating the market and also business demand will be low. Opportunities for new vendor solutions to scale up will therefore be severely limited, which is also seen as a requirement for granular solutions to catch up with traditional ones. A challenge of open architectures is to meet the stringent requirements that vertical applications have (in terms of latency, bandwidth, jitter, reliability, etc.) with general-purpose computing and COTS solutions in a cost-efficient manner. Under this scenario, this challenge would be virtually unsurmountable even with a 2030 horizon.

Concerning the demand side, the capabilities of MNOs to thrive in the enterprise segment will be challenged by the capabilities of their competitors. These include use-case specialised MVNOs and other players, including Big Tech. This represents an additional threat to MNOs, on top of the inherent threat in this scenario which is the hypothetical slow rollout of 5G due to lack of consumer demand. To respond to both, MNOs may aim at adopting a 'Use case enabler' business model (Camps-Aragó, Delaere & Ballon, 2019). This consists of developing comprehensive and tailored solutions for specific use cases, to speed up their adoption and valorise an early position. To do so, operators

68 The full analysis of the baseline assessment can be found here: https://zenodo.org/record/4621102/files/5GSupplyMarketTrends_BaselineReport.pdf

have to, first, enhance the value proposition of public networks, for instance by offering a tailored network slice and equipment that covers the specific requirements of the use case. Second, this model entails offering additional services such as deployment support or technical advisory (e.g., regarding the integration of components), which would be based on the data and expertise gained across deployments of the same use case. This would allow vertical market companies to focus on their core businesses. However, because building the necessary vertical-specific expertise entails specialization efforts, it may only be feasible for each operator to target a handful of use cases.

Scenario III: Open RAN as a game-changer

In this scenario fully virtualized networks that rely on open, standardised, RAN interfaces become reality, resulting in highly competitive 5G supply markets with many small and competitive entrants spurred also by high demand of the vertical industry. Therefore, this scenario is where the system integrator (SI) business model options peak in relevance.

In this scenario, the need for system integration expertise is high. New players, which offer technology-based innovations for digital transformation, are gaining importance and position themselves as integrators. Therefore, this scenario is where the system integrator (SI) business model options peak in relevance. The successful introduction of RAN openness is being accompanied by different SI models that may be used by new vendors. Leaving market readiness aside, the uptake of Open RAN rollouts will depend on the predominant SI business model.

MNOs may still need integrated solutions if they do not build up the required knowledge capacity along the process. White boxes based on open-source provided by new entrants will be most likely in this scenario, due to the quickest and farthest-reaching entry of new players, the maturity of standards, and the high R&I investments and policy support for new actors in Europe.

Despite this, traditional vendors could take early leadership in Open RAN and make sure new players develop under their leadership. Since new players will not be able to compete on costs with established vendors at the beginning, such vendors will have the opportunity to orchestrate integration efforts and even acquire innovative players. On the contrary, if they don't adapt timely, they face the threat of being overtaken by more innovative players as soon as rollouts based on Open RAN interfaces reach scale. Also, the traditional black-box model may probably remain in existence for several years, even in this optimistic scenario. As mentioned for cost and competition dimensions, Open RAN solutions are not expected to be economically mature and widely adopted in the market until at least 5-6 years from now.

Scenario IV: 5G for Big Tech

In this scenario, the SI role is being taken by the GAFAM via the outsourcing model. This poses a threat for European industry, as foreign Big Tech players, relying on their strong capabilities in automation, cloud (back-end, data centre architectures, etc.) and analytics, become the go-to integration option and establish a strong grip over the value created in the entire supply chain.

In this scenario, respondents argue that software-based solutions push integration, and IT-savvy companies may be better poised at integrating virtual RAN components. On the other hand, other respondents question whether Big Tech companies have an incentive to play this SI role. Today, their focus seems to fall on partnering with traditional vendors.

On the demand side, the threat is similar, which highlights the potential of Big Tech players to achieve concerning dominant positions in this scenario. MNO's business models have been undermined by OTT applications due to the trend towards software-based solutions, from voice calls to messaging, to content platforms. Big Tech companies have stronger capabilities than MNOs to offer end-customer OTT services, which target the most valuable layer of the demand-side value chain. Moreover, their cloud-based platforms give them the ability to cross-subsidise across their product portfolio.

Based on our interviews, we could identify the following threats for MNOs. In the B2B connectivity market, MVNOs or Big Tech companies who innovate at the application layer may take over MNOs market shares. Some IoT MVNOs are already competing successfully for certain use cases (e.g., Transatel with connected mobility), even though they do not own the network. This example shows that competing on costs is not enough for connectivity service providers to have a competitive advantage in some use cases where network requirements are challenging and distinct. The key potential for Big Tech is that they are better at software and IT integration, and an understanding of and covering the needs of industrial customers. While this shakeup is not necessarily a threat for Europe —on the contrary, it may incentivise innovation—, a related threat is that this market disruption is brought by foreign tech players, who could potentially build up the same kind of capabilities.

To address these threats, MNOs need a change in mindset: rather than conservatively focusing on the mass market and on selling capacity, shift to a more service-led approach for verticals and adapt existing business models to tackle new services for B2B use cases. A specific example of a business model was described for Scenario II.

Regarding opportunities at the supply side, an interesting business model is to become a B2B focused MNO. Recently, the IT company Cegeka and the MVNO Citymesh joined forces to become the fourth Belgian MNO, with a specific B2B focus.

e. Supply of new services and applications

Current situation and sources of impact

New services and applications based on 5G and the evolution of 5G networks are interrelated. On the one hand, mobile service operators will roll out and improve their 5G infrastructure only if they can draw enough customers into new services that rely on 5G and cannot be realized with 4G. This was the case with data communication and video streaming for 4G. The applications which have driven 4G traffic may create too little additional demand to push 5G. On the other hand, a lot of new services may not be possible without the higher bandwidth and lower latency rate of 5G. 5G will not come to real life when services that make use of its superior technological features are not available and thus do not give additional value to firms or the customer. The emergence of new services and applications based on 5G thus appears as a 'Chicken-Egg problem'. This search for a 'killer app' has accompanied the introduction of each new mobile standard so far.

This dilemma can be solved by stabilizing and aligning the expectations of each market participant. This can be done by rollout plans with comprehensible milestones at the side of mobile service operators, or with 5G demonstration projects trials. According to one interview partner, 5G infrastructure and 5G services will most likely develop co-evolutionary in the next years. Covid-19 has delayed many trials by one to two years.

The appeal of 5G for new services lies in the superior technical features of this technology over 4G, in particular.[69] 5G allows:

- real-time communication with a very low latency time and high availability of service; moreover, latency is independent of the number of devices in one cell;
- a considerably higher bandwidth, so services can send and receive much more data than in a 4G RAN;
- network access to considerably more connected devices in an area than 4G;
- to transfer small data packages by devices that require far less energy for this task than 4G, thus allowing devices that are not dependent on frequent recharge.

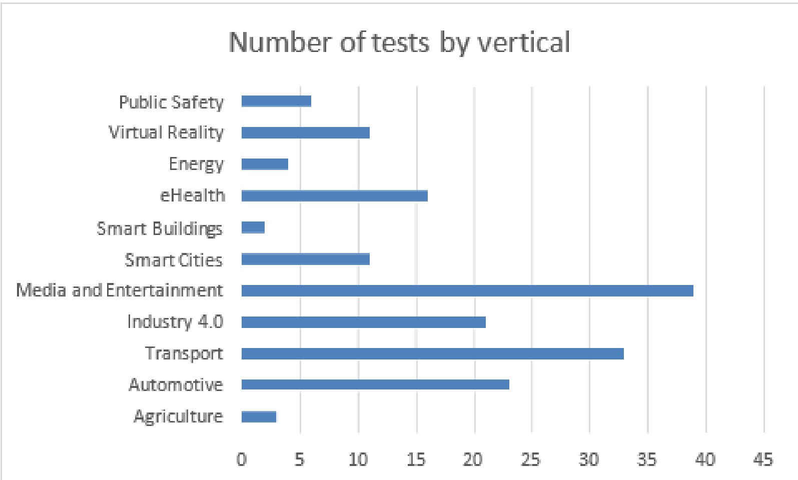
69 Ullah et al. (2019)

But innovation is not just about superior technology. History provides many examples of new products that did not meet the expectations or even failed on the market, from MMS to Windows Mobile. Innovation is not shaped by technological opportunities alone, but also by market acceptance, a lack of skills, the availability of supporting infrastructure and appropriate business models, appropriability and lock-in effects etc.[70] In many countries, telecommunications services have become a commodity in the last ten to 15 years, and mobile service operators have seen their margins fall, rather than rise. This reduces the willingness of consumers to pay a premium for new services

Ahn et al. (2005) have analyzed failed telecom innovations in Korea. They identified ineffective marketing activities, poor demand forecasting, failure to satisfy technical specifications and poor quality, loss of cost advantage due to the price cut of competing services or lower-priced new entries or loss of utility advantage due to the moves of competitors, as reasons these failures.

Moreover, several services can be implemented based on different technologies – 5G, 4G, WiFi, or a mix of these technologies. An example is IEEE 802.11p, a standard for wireless access in cars based on WiFi (IEEE 802.11) that is currently implemented at Austrian motorways[71]. Thus, we should think about features of services independently of the underlying technology, and the selection of technology should depend on the specific application conditions. This is one strength of 5G, which is very adaptive to the specific needs and can be configured to provide more latency, bandwidth, etc. when it is needed.

We think it is important to consider these obstacles when discussing possible new services based on 5G (use cases). The academic literature on use cases is scarce (an exception is Ullah et al. 2019) which reflects the timeliness of the topic. The European 5G observatory, a project supported by the European Commission, provides a comprehensive list of 5G trials and the respective application sector (vertical) in the EU27, UK, Norway, Russia, Switzerland and Turkey[72]. As of December 2020, 245 trials have been identified, with media and entertainment (39 trials) being the most frequent application area, followed by transport trials (33) and trials in automotive (23 – see Figure 3). A couple of these trials, however, cover several application areas.



Source: European 5G Observatory, quarterly report 10

Figure 3: 5G trials by vertical (sector), December 2020

70 Cohen (2010), Pavitt (2005)
71 https://www.c-oads.eu/fileadmin/user_upload/pics/News/PA_ASFINAG_Connects_Roads_with_Vehicles.pdf
72 http://5gobservatory.eu/5g-trial/major-european-5g-trials-and-pilots/

Media and Entertainment is the most frequent use case in 5G trials according to the Observatory. This includes live events, as well as streaming of video and audio data and applications of augmented reality.

Live events are relevant for 5G because of their ability to deliver services to a large number of devices in a small area. Data volumes consumed by spectators of soccer matches in the arenas of the German Bundesliga increase by 50 to 60% each year, which can only be satisfied by 5G technology[73]. Vodafone is currently installing a 5G network at the stadium of Wolfsburg, a club in Germany's Bundesliga, to explore applications of 5G for live events. Possible use cases include interactive services and virtual reality, which may even increase data demands.

Video and audio streaming and non-linear broadcasting were some of the most important drivers of the diffusion of 4G. It may also promote 5G due to higher bandwidth. However, due to the high capacities of existing 4G networks, it seems unlikely that video and audio will play a similar role for 5G. Only new, more interactive services including virtual reality may justify 5G bandwidth.

Applications of 5G in ***transport*** include Connected and Automated Mobility (CAM), drones, real-time tracking, or traffic management systems. Real-time data is highly relevant for many transport applications because of security. Thus, transport services can benefit from the high availability of service, very low latency of 5G, and require high-security standards.

Connected and Automated Mobility (CAM) in the form of autonomous vehicles received the most attention so far (Boban et al. 2018). Trials are currently run by most automobile companies. Perhaps best known are the trials by Waymo, a subsidiary of Google, and by Tesla.

CAM includes various levels of automation[74], with different communication needs. The highest levels 5, 6, and 7, where driving tasks are performed automated at least for some time, multiple types of communication with its environment, including vehicle-to-vehicle, vehicle-to-pedestrian, and vehicle-to-infrastructure communication are required, and all of them are highly safety-relevant. This requires very low latency times of around 1 ms and very high bandwidth, both of which can only be provided by 5G. Intel, who has teamed up with BMW and Fiat to develop CAM, estimates that the sensors of a driverless car will generate around one GB of data each second[75]. To put this number in perspective, subscribers of mobile services downloaded on average 5.8 GB per month in the OECD 2019[76]. So, even if only a fraction of the data generated by CAM needs to be transmitted, the required volume will exceed today's available capacities by far.

Ambitions to bring CAM finally to the market, however, seemed to have cooled down recently. At the end of 2020, Uber, supposedly one of the biggest beneficiaries of the technology, decided to cancel its plans for self-driving taxis[77].

To date, it cannot be predicted when the driverless car finally will hit the road. ERTRAC a European Technology Platform (ETP) for Road Transport, expects fully automated passenger cars, not before the end of this decade and some lower levels of automation including urban and sub-urban Pilot around 2024-2025[78]., according to one interview partner, technology is not the main bottleneck: rather, the activities of carmakers, providers of infrastructure and mobile network operators need more co-ordination, and investments and regulatory frameworks across the EU need more convergence. The proposed Joint Undertaking on Smart Networks and Services towards 6G can be one frame for such coordination.

73 https://www.handelsblatt.com/technik/it-internet/bundesliga-vodafone-ruestet-wolfsburg-stadion-mit-5g-aus-videobeweis-fuer-zuschauer-moeglich/24518906.html?ticket=ST-8063510-Akr4ZEmMKAIPSEonyd6f-ap5
74 https://saemobilus.sae.org/content/j3016_201806
75 https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/automotive-autonomous-driving-vision-paper.pdf
76 http://www.oecd.org/digital/broadband-statistics-update.htm
77 https://www.theguardian.com/technology/2021/jan/03/peak-hype-driverless-car-revolution-uber-robotaxis-autonomous-vehicle
78 https://www.ertrac.org/uploads/documentsearch/id57/ERTRAC-CAD-Roadmap-2019.pdf

It seems clear that CAM will have very high requirements to 5G infrastructure; however, a broad market introduction of CAM cannot be expected within the next 5 years, so it's unlikely that the data requirements of CAM will be an important driver of 5G rollouts. Rather, CAM may be a driver of 6G and other future mobile communication technologies.

Another potential field where 5G can play out its strengths is *drones*. Application areas include drones for delivery, agriculture, communication, surveillance, technical inspection, disaster recovery, and even passenger transport. Drones for commercial applications are already in production, while regulatory issues including air traffic safety are still open in most countries.

A drone will have some degree of autonomy but will require wireless communication. For example, delivery drones that operate in a small urban area require remote control and very low latency. Inspection and surveillance drones have to be able to transmit various types of data. Interview partners think that drones may develop into an important use case for 5G.

The Internet of Things (IoT), or Industry 4.0 in the German context, refers to the integration of production activities within the factory and along the supply chain by exchanging data between the various stages. Networked equipment and sensors attached to goods provide data that is used by management systems to coordinate the different stages. IoT implies that the largest part of communication in 5G will take place between machines (m2M), and it may also include communication between autonomous devices. Production coordination may also be a future application field for artificial intelligence. Another potential technology that may emerge in the context of Industry 4.0 is autonomous robotics.

IoT requires ultra-reliability and low-latency 5G networks and may also combine 5G and WiFi within factories. According to the interview partners Industry 4.0 is an area where some of the most innovative developments are currently taking place. An example is Cellnex' installation of a private 5G network for BASF, a chemicals company, in Tarragona, Spain. The project will include applications of the Internet of Things (IoT), the implementation of big data, virtual and augmented reality and artificial intelligence.[79] Another example is the 5G private network installed by Hutchison in the port of Felixstowe, UK, where 5G is used for communication and also for remote piloting of cargo handling[80]. Private networks can provide 5G access in confined areas such as factory shop floors, industrial areas or ports well before the rollout of 5G is finished. These confined areas may also provide the ideal environment for the first real-world applications of CAM, for example for automated materials handling.

Interview partners consider IoT currently as the main use case within 5G, followed by drones and health. They expect that IoT will consume the largest chunk of 5G capabilities over the next years.

Finally, ***health*** has become a field where many expect important applications of 5G in the future. The case for 5G in health emerges from human interaction and the fact that health services require that the patient and the practitioner are in the same place. If 5G can bridge the distance between patient and practitioner being in different places, more people may get better treatment or, any treatment. Moreover, online health services may provide better regulatory governance and transparency because it would facilitate documentation (Caric et al. 2015). Another advantage is that data collected by online health monitoring can be analyzed by artificial intelligence in combination with human expertise.

A major push for 5G use cases in health comes from the Covid-19 pandemic, which has changed the attitudes of the population towards patient-oriented health applications (an example is a software that traces contacts) or online consultation and led to massive public investments in digital health

79 https://www.cellnextelecom.com/en/basf-and-cellnex-will-bring-5g-technology-to-the-tarragona-production-centre/
80 https://uk5g.org/5g-updates/read-articles/port-felixstowe/

technologies. Ullah et al. (2019) describe four possible health use cases: online consultation, online health monitoring, remote diagnosis and remote/robotic surgery.

Online consultation includes communication between patent and practitioner, while online health monitoring includes the automatic collection and transfer of patient data. Both types of services are likely to be combined. Remote diagnosis refers to long-term surveillance of patients who may suffer from chronic diseases like diabetes or chronic heart failure. Remote or robotic surgery is the most advanced type of 5G use case where patients are treated remotely. Haptic sensing, ultra-low latency and high-security standards are essential here. Low latency and high security are, of course, also important for the other forms of online health services.

Scenario-specific assessment

How are the services or use cases linked to the four different scenarios developed in the project? Do some scenarios provide better opportunities for particular use cases? These differences may be related to a better fit between technology and service, to new players that driver particular use cases, etc. Use cases and 5G roll-out may also interact with each other so that new use cases demand a faster roll-out, or new 5G capacities may facilitate services development.

Scenario I: Incumbent players driving 5G

Here, incumbent MNOs and vendors orchestrate the emerging 5G innovation ecosystem and provide a smooth transformation from 4G to 5G. Such a surrounding is conducive to the development and introduction of new services since it offers security and stable relations between MNOs and their retail customers.

However, incumbent MNOs with their focus on hardware may not the best actors to introduce new services. The decade-old search of MNOs for a ‘killer app’ that pushes demand for new generations of mobile communication is a testament to this claim. For 4G social media and software companies such as Facebook, Google or YouTube introduced the services which drove the growth of mobile data.

We may therefore expect that services will emerge which are a continuation rather than radical departures from the existing services. This may include media and entertainment, transport information systems, or IoT applications. Health applications may benefit in particular because the eco-system of Scenario I – with MNOs that have a proven track record - provides the security necessary for such applications to flourish.

Scenario II: Slow pace of 5G Roll-Out

A lower number of potential suppliers and slow 5G diffusion, in turn, most likely indicate high 5G service charges for consumers. It seems unlikely that we see rapid development and market introduction of new 5G based services in such an environment. Moreover, segmented geographical markets may further hamper the roll-out of Europe-wide services.

At the level of individual use cases, we believe that services with the highest capacity requirements – CAM, drones and health – will suffer most in this scenario. Services which emerge from existing 4G use cases such as entertainment are more likely to develop in such an environment. Industry 4.0 seem to be unaffected by the adverse development of as long as 5G connectivity is only required in a restricted area of an industrial facility. Here, 5G services in customized installations can excel.

Workshop results point to the fact that security may be stronger in Scenario II than in other scenarios. Hence, this may be an appealing scenario for mobile, 5G-based health services, in particular when national public policy pushes their introduction. However, as noted above, health services may also be hampered by a lack of performance and too low diffusion of 5G in this scenario.

Scenario III: Open RAN as a game-changer

Decentralized, disaggregated and fully virtualized Open RAN networks serve Europe in this scenario. This is a favourable starting position for new 5G-based services particularly for vertical industries and more advanced use cases (e.g. health, Industry 4.0). For the end consumer markets the impact of Open RAN is more likely less relevant. High levels of competition and new network operators will lead to low prices and a high willingness for innovation and experiments in the market. More suppliers in the vendor ecosystem also allow deploying customized networks for different user groups (e.g. industrial facilities). Moreover, interoperability between European countries facilitates the Europe-wide rollout of use cases.

Such an environment favours new, data-intensive services in particular, and we expect that drones, CAM or the Internet of Things and health will benefit in particular in Scenario III. Security for e-health and CAM applications is sufficient in this scenario, so it cannot be an obstacle to roll-outs. It seems also likely that even new services where no use cases exist so far will emerge in this scenario. Market entry of new players who serve as operators will give services development a new push because these firms will bring in new perspectives on what can be done with 5G. Moreover, market entrants from different sectors (verticals) that provide new services are also likely, for example by firms from different manufacturing sectors which enlarge their traditional offers with new, 5G based services. Europe has some particular strengths in manufacturing, for example in machinery, transport or aerospace, so it may be that new entrants come from these sectors and not necessarily from ICT or telecommunications.

Scenario IV: 5G for Big Tech

Here, Big Tech companies conquer the 5G supply markets with Open RAN business models and become new, virtual MNOs. Such a scenario is very appealing from a use case perspective because the services of Big Tech companies drove the demand for 4G. In the past, Big Tech companies proved their ability to integrate various technologies into very appealing consumer services. The most obvious examples are Apple and Amazon. Moreover, new market entrants are likely to drive prices for 5G services down.

A use case that would benefit in particular in such a scenario is Connected and Automated Mobility (CAM). Google, Amazon and Apple are very active in developing CAM, and also have the financial means for massive investments in 5G infrastructure. These firms may even have higher incentives from increasing returns from 5G infrastructure investments, as not one, but several of their services would benefit from them. However, European car manufacturers would also benefit from these investments, maybe in co-operation with US tech firms. Another area where use cases may benefit from complementary competencies within Big Tech companies is health; there seem to be strong additionalities between artificial intelligence and health applications. However, we also know that US Big Tech companies have a different approach to privacy and security than European regulators. This may be an obstacle to a wide diffusion of 5G-based health services, as many consumers in Europe may be hesitant to offer their health data to US Big Tech companies.

Prospects for European firms may look less bright than in Scenario III because US Tech firms may prefer to develop closed service environments which they can control; however, European employment and value-added (but not necessarily European-owned firms) will also benefit from such a scenario when US Tech firms provide services through European subsidiaries and these services are taxed accordingly. Altogether, Scenario III and Scenario IV may provide the most favourable environment for the emergence of new 5G-based services. Scenario I can be regarded as neutral and a continuation of today's environment, while Scenario II seems less favourable for new services.

f. Modularity and supplier dependency

Current situation and sources of impact

By increasing competition, pushing for more open interfaces and embracing open-source, MNOs are seeking to reduce the dependency on a reduced number of traditional vendors. However, opening interfaces also raises several concerns. Below, we present a discussion that covers several issues, including the expected impact of disaggregation on supply chain resilience and European sovereignty.

Digital sovereignty

At first sight, it is not clear whether a thrive for opening up interfaces will increase the digital sovereignty of Europe. And since we are talking about critical infrastructure in many cases, this is an important discussion. There exists the threat that Open RAN will increase European dependency on foreign components (e.g., microprocessors and cloud infrastructure) while weakening the current dominant position of European vendors. In sum, Open RAN represents both an opportunity and a threat, and the resulting impact is expected to depend on market evolutions and, even more so, on policy measures.

Vendor lock-in

The main current concern of MNOs is being stuck with a reduced number of suppliers for the RAN, after a potential geopolitically motivated exclusion of Huawei and a trend toward industry consolidation during the last decade. The reliance on few vendors not only reduces the bargaining power of equipment customers but also lowers the resilience of the overall supply chain, as the risk of a supplier lagging in performance or suffering some kind of financial or operational disruption is always present.

Open interfaces would allow operators to replace any discrete component at different points in time, without depending on a single vendor per part of the network and per region for the entire “generation”, as is usually the case with current business models (see the section on ‘business models’ for an in-depth discussion on this). Open interfaces would also allow MNOs to rely on a different vendor when choosing to replace a specific RAN component.

Relatedly, the use of white-box solutions would allow customers to understand what elements are inside the box and understand the protocols via which the different interfaces communicate, something that, according to several of our interviewees, it is not possible today. With open architectures that rely on open-source software, RAN customers could audit a certain chip or piece of software and its source code.

Specifically, at the software layer, supplier dependency would be reduced in case the use of open-source becomes more common in building software products. Nevertheless, with this and other business models based on multi-vendor pre-integrated solutions, the threat of system integrator lock-in appears.

Potential adverse effects from disaggregation

It is also important to keep an eye on potential new bottlenecks, as well as potential lock-in to new types of dominant suppliers. We briefly consider four main issues: 1) cybersecurity threats, 2) supply chain resilience, 3) new bottlenecks and 4) higher dependence on foreign players.

Even though technical analysis is out of the scope of this section, cybersecurity is a relevant aspect to consider for the analysis of this impact dimension. As one demand-side respondent put it, “in the end, many operators started looking at Open RAN because of the implementation of the 5G cybersecurity toolbox, which resulted in concerns and even potential bans on Chinese providers”. Several respondents showed concerns about the potential adverse effects of disaggregation on the security of the networks (see below).

Regarding supply chain resilience, concerns include the potential disruption caused by the need to replace one of the vendors (either software or hardware). Multi-vendor environments will imply smaller vendors, the stability of the business of whom is also a question. As after-sale services and life-cycle product management are required, the concern is: ‘What will happen if a supplier goes bankrupt or abandons the market?' Therefore, the risk of disrupting the entire chain in case one element is dropped needs to be avoided.

A further issue is the risk that the opening of RAN interfaces moves the problem of bottlenecks elsewhere in the supply chain. A shift toward supplier dependency at the chipset level was the most commented concern, as more open or virtual radio networks will still have hardware dependencies coming from processors.

One cited threat arises from smaller companies not having the capabilities to compete in chip designs versus big firms. Traditional vendors urged to not underestimate potential market dominance at the silicon layer of the supply chain. As is the current case with RAN vendors, this dependence on a dominant supplier would make the entire supply chain more vulnerable. An MNO also mentioned that there currently exists a lock-in to Intel's x86 regarding silicon. This is because they do not only provide the processor but also all the support services around it: complete SDKs, engineering support, the accelerators cards needed to run the workload for base stations, etc. However, there was disagreement in this regard amongst our interviewees. First, because there are many chipsets suppliers in the RAN space: Qualcomm, NXP, Broadcom, Intel, Marvel, etc. and many start-ups are expected to enter the market as a result of Open RAN, as several are already working on it (this was mentioned in the 'competition' section). While nowadays there is a strong dominance of Intel for Open RAN, this is expected to change. Intel realised the potential of Open RAN early on and started working on it before its competitors.

Another concern is that leading chipset players are not European. This concern was raised independently of whether respondents were worried about potential dominant oligopolies at the chipset level or not. Currently, there are not many strong providers in Europe in the semiconductors field. On the contrary, Chinese and American designs dominate the market.

Relatedly, another cited problem concerns the manufacturing of chipsets, hence, the location of silicon foundries. Currently, Europe also relies strongly on international manufacturing. Having diversification in terms of producing regions for semiconductors is seen as a source of supply chain resilience and digital sovereignty.

Lastly, another related issue concerns availability. Since the Covid-19 crisis, there has been a global shortage of chips. There are concerns that this shortage may last beyond the short term. One source of the issue is that with the IoT, and the resulting much higher amount of intelligent devices, more chipsets are needed. Therefore, there is a perceived need for higher manufacturing capability to keep up with demand to guarantee the resilience of the supply chain at the chipset level.

While the growth of the 5G era brings the opportunity for new business models and European companies to emerge, the overall view was that policy action is needed. Nevertheless, this is already in the making. The EC recently announced the Digital Compass which covers the challenging ambition of doubling European market share for semiconductors in 2030 and of having manufacturing capabilities for 5, 4 or even 2 nanometre chips.[81] Moreover, a recent joint declaration by 21 Member States shows the commitment to reinforce the European processor and semiconductor ecosystem and to advance European chip design and production capabilities.[82]

Finally, the potential adverse effects from a higher dependency on foreign (i.e., non-European) players on the software layer need to be considered. As mentioned for semiconductors, the presence and capabilities of EU players in software or cloud infrastructure are limited, when compared to current market leaders. This adverse effect mainly comes from the related, existing trends of virtualisation and moving network functions toward the cloud. Nevertheless, the opening of RAN

81 https://digital-strategy.ec.europa.eu/en/policies/digital-compass
82 https://digital-strategy.ec.europa.eu/en/news/member-states-join-forces-european-initiative-processors-and-semiconductor-technologies

interfaces is seen as an indirect driver itself, by stimulating the entry of new players in a disaggregated radio network with decoupled software and hardware.

- Big foreign internet companies have the potential to become very dominant throughout the chain. While the entry of these ‘GAFAM’ players as telco infrastructure providers, selling services to MNOs, is still uncertain, they want to host intelligence in their cloud platforms and control the application layer. Moreover, their current market movements (for instance, the recent announcements of Nokia cooperating with them), points at a supply chain with more presence of US companies. Moreover, the business models of GAFAM are based on allowing third parties companies to develop solutions based on the application level but keeping control on the host infrastructure. Therefore, a potentially strong presence of Big Tech in Open RAN poses a threat to the bargaining power of European MNOs and vendors.
- Several interviewees argued that boosting the entry of GAFAM would undermine EU sovereignty. Similar arguments to those made to avoid depending on Chinese companies could also be used for American ones since they have also been involved in geopolitical scandals in the past (e.g., concerning espionage on European actors). One interviewee voiced a related concern: underlying the US push for Open RAN there is the geopolitical-economic purpose of enhancing the global competitive advantage of US companies while promoting technical decoupling from Chinese products for US and European companies. The resulting ecosystem, in case Chinese companies are excluded due to geopolitical decisions, would create an opportunity for US companies to take more control of the supply chain (both for software as well as for the chips).
- Other respondents noted that Open RAN will happen with or without European leadership. In that case, MNOs reiterate the importance for European vendors to adopt Open RAN to adapt and maintain a competitive position. Whatever the impact from Open RAN would affect them anyway, as a large part of their business happens outside of Europe. Based on that view, it would be more sensible for Europe to take leadership in an Open RAN scenario, as not doing so would weaken the continent’s position in any case. To avoid the dominance of leading foreign software companies, the main policy recommendation was once again to foster an ecosystem of European companies (in this case, tech companies).

Scenario-specific assessment

Scenario I: Incumbent players driving 5G

In this scenario, large MNOs and incumbent suppliers play a strong role. While incumbent MNOs build up the needed capacities to increase their bargaining power vis-a-vis incumbent vendors, the overall pace of modularisation and decrease of supplier dependency is medium.

Due to their knowledge capacity, traditional vendors can to some extent orchestrate the development of the new ecosystem, but their business models and price policy needs to be adjusted as new alternatives emerge on the horizon.

Scenario II: Slow pace of 5G Roll-Out

The most pessimistic scenario is characterized by a modest if not negligible change for the adoption of more modular networks. The rollout of open and interoperable 5G network solutions is slow, which results in the likely outcome of traditional, integrated vendor solutions dominating deployments. 5G rollouts stagnate and look like those we are witnessing today, which rely on traditional use cases and traditional vendor solutions. Therefore, this scenario portrays a concentrated supply market resembling the status quo. As a consequence, the issues regarding vendor lock-in are assumed to persist, while the potential adverse effects from disaggregation remain just a threat for the even more distant future.

Scenarios III & IV: Open RAN as game-changer & 5G for Big Tech

We provide a shared assessment of Scenarios 3 and 4. While yielding strongly differentiated outcomes, many of their underlying trends are shared, and our discussion will mainly focus on the trade-offs between the two, and on how a specific outcome will be influenced by policy.

Both scenarios assume the following: (i) a rapid uptake of open and interoperable 5G RAN solutions, (ii) high entry of new players, (iii) extensive increase in Research & Innovation (R&I) investments in the EU, and (iv) moderate security challenges due to the opening of RAN interfaces and the resulting diversification of the supplier ecosystem.

Where they differ is in the two following points:

- Policy support for pilot projects in collaboration with verticals. While Scenario 3 is the result of years of policy support for strong 5G use cases, Scenario 4 lacks this political support. It is assumed that this is a main cause for the distinct outcomes in terms of competition.
- Open RAN standards development. In Scenario 4, this development is led by Big Tech companies, while in Scenario 3 it is more universal, with more presence of smaller players and more focus on open-source.

Policy support for pilot projects in collaboration with verticals and new actors is seen as key to avoid a scenario with more dependence on foreign suppliers. As we discussed before, there is a current dependence on foreign players for software and silicon chips. The threat of this dependence being exacerbated in the future is present in both scenarios. In Scenario 3, even with a more competitive market, the source of the threat is that the entrance of new foreign players reduces the market shares of current EU players. In Scenario 4, the cause of the threat is a more dominant position of software and cloud providers, in the form of Big Tech players.

In scenario 4, higher competition at the supplier level offers an opportunity to operators to reduce their current vendor lock-in. However, there is the threat that incumbent vendors and Big Tech players partner to divide market segments between them. They could partner to offer proprietary solutions in which the incumbents take care of certain elements (e.g., providing on-site equipment) and tech players offer complimentary ones (such as the processing in their cloud environment). Such an approach could likely be a dominant one from early on and represent a barrier for entry to new players. There is a similar, additional threat that MNOs become specifically locked into GAFAM's solutions, creating a new bottleneck at the cloud level**.** This also represents a threat for vendors, as foreign internet companies could exert influence throughout the chain, especially due to their dominance at the core, and appropriate a higher share of the overall value created at the supply side.

Avoiding the potential negative outcomes of both scenarios means boosting competition and the presence of European players at the same time. The main recommendation for policymakers from our interviewees is that the EU helps to build and scale up an ecosystem of European suppliers. Such an ecosystem would have the objective of stimulating the growth of smaller/new EU companies to become worldwide leaders in each specific element. While some MNOs argued in favour of public funding to set up European R&D projects, other respondents preferred that funding is used to ensure that SMEs have access to early-stage private investment, for instance by setting up funds managed by venture capitalists, so that the choice of which projects to fund is done by private investors. It was also argued for, and against, protectionist measures to make sure successful EU companies are not acquired by foreign players.

Regarding digital sovereignty concerns, Scenario 4 poses an obvious threat. The higher dependence on foreign players on the software layer would undermine EU sovereignty in this scenario, according to most of our respondents. Assuming their entry as telco infrastructure providers, foreign internet companies would become very dominant throughout the overall value network, including on the end customer side, where they compete with MNOs. According to several respondents, European vendors would relinquish control over the supply chain, lest they adopt Open RAN. However, others argue that they could still maintain a competitive position on certain domains, such as RAN equipment, since tech companies focus mostly on the core, and are currently opting to partner with vendors for other elements.

Stemming from the assumptions regarding standards development, Scenario 4 poses a threat if these players offer proprietary solutions that are compliant with different standards than the ones being developed in current initiatives. Over time, different non-interoperable software-based solutions could dominate the market.

Regarding supply chain resilience, concerns include the potential lack of stability of smaller entrant suppliers, due to their financial viability or cybersecurity concerns. Scenario 3, which implies multi-vendor environments with a higher presence of smaller vendors, would offer the biggest threat in this regard.

g. Cybersecurity

Current situation and sources of impact

The 5G security architecture is defined in the 3rd Generation Partnership Project (3GPP) technical specification as having six main domains: network access security, network domain security, user domain security, application domain security, service-based architecture domain security, and visibility and configuration of security.[83] Therein, several potential cybersecurity opportunities risks that are likely to be intrinsic to 5G networks regardless of vendor or operator are being put forward.[84] Examples of risks shaped by specific actors are likely to be the lack of diversity in the 5G supplier base, whilst risks intrinsic to 5G networks are likely to include a shift from a hardware focus to a distributed software focus, growth in the attack surface, and the use of machine learning to scrutinize data that may be private or confidential.

Such risks have led to specific, targeted initiatives to address 5G cybersecurity risks. For example, in 2019, the European Commission adopted a recommendation regarding the cybersecurity of 5G networks. This called on the Member States to complete national risk assessments and review national measures, to work together at the EU level on a coordinated risk assessment, and to prepare a toolbox of possible mitigating measures. The objectives of the toolbox are to identify a potential set of measures that can mitigate the main cybersecurity risks of 5G networks and provide guidance for the selection of measures that should be prioritised in mitigation plans at the national and the European Union level. In doing so, the toolbox aims to create a framework of measures to ensure an adequate level of cybersecurity of 5G networks across the EU and coordinated approaches among the Member States.[85]

Concerning the lack of diversity in 5G suppliers, path dependency weakens the resilience of networks – and 5G currently relies predominantly on three suppliers: Nokia, Ericsson, and Huawei.[86] Although such a scenario promises effective economies of scale in 5G network deployment, according to the interviews there was both a greater degree of competition and greater diversity of companies for the roll-out of 2G, 3G, and 4G networks. Dependence on single-vendor solutions across the entire network ecosystem for 5G, although it may prove cost-effective for operators, also increases the risk of exposure scaling across a wide length of the network in the event of a cybersecurity attack.

This risk of dependence on a single vendor could play a role in the 5G network market.[87] In such a scenario Open RAN could prove to be a potential solution to reduce the dependence of operators on a single network equipment vendor.[88] However, opening up of the interfaces and the need for

83 Suomalainen *et al.* (2020)
84 Griffith (2020)
85 NIS Cooperation Group (2020)
86Peters and Besley (2019)
87 RWR Advisory Group (2021)
88 Griffith (2020)

increased system integration due to Open RAN may create a new set of security challenges. The work on Open RAN specifications in this security context is ongoing and would need to be carefully monitored to identify and respond to threats effectively.

5G network moves away from a centralized hardware-based approach to a distributed software-based approach. In previous generations of wireless networks, the hub-and-spoke design meant that hardware 'choke points' could ensure that cyber hygiene could be practised, and which offered the potential to halt malicious cyber-attacks. As 5G is software-defined, it denies these chokepoints for inspection and control and may leave cybersecurity vulnerabilities.[89] While the cybersecurity arrangements of virtualized networks are more flexible and scalable than physical hardware infrastructure, the risks posed by this could increase as software code can be configured and combined in unexpected and unanticipated ways.[90]

Machine learning – which is hoped to solve many of the challenges facing 5G – could inadvertently open the network to cybersecurity vulnerabilities.[91] Machine learning requires algorithms to learn from data in the environment – but where un-scrutinized data reduces the ability of algorithms to provide meaningful insights, scrutinized data opens it up to cybersecurity challenges such as leakage of private and confidential information. The main threats of machine learning to 5G are Denial-of-Service, Denial-of-Detection, unfair use of resources, leaking company secrets, and privacy leakage – see Figure 4. Vis-a-vis Open RAN specifications, the use of Machine Learning (ML) is mainly in the RAN Intelligent Controller (RIC) which is intended to support interoperability across different hardware and software components to optimise resource usage and deliver the best possible Quality of Service (QoS) to the subscribers. As of early 2021, the work on RIC in the Open RAN specifications is still at relatively early stages so the cybersecurity risks and opportunities are not yet fully understood.

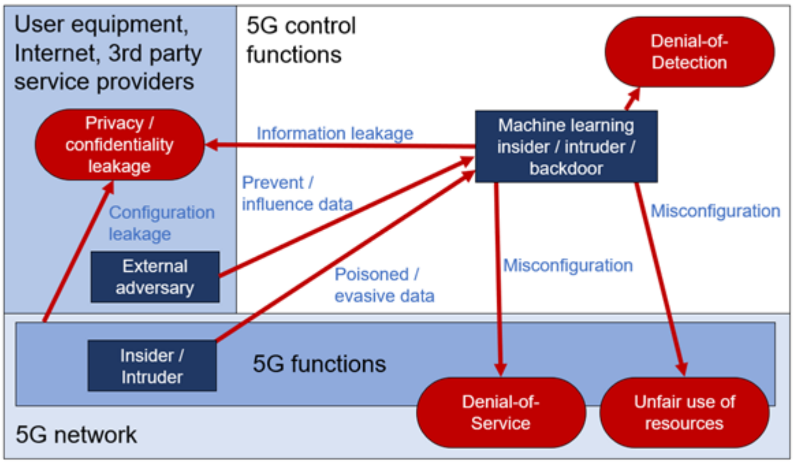


Figure 4: Potential threats for 5G[92]

The increased connectivity offered by 5G and increased dependency on the network could also enlarge the attack surface for potential adversaries and hostile agents.[93] According to interviewees, some states have already noted their dependency on 4G RAN. A slow or interrupted 4G network may result in problems such as slower downloads of email attachments or loading of videos. The multitude of prospects offered by 5G, including smart grids, remote surgery, driverless cars, and the Internet of Things (IoT), increase the potentially larger scope for network outages. From such a

89 Wheeler and Simpson (2019)
90 Oxford Analytica (2021)
91 Suomalainen et al. (2020).
92 Adapted from Suomalainen et al. (2020)
93 Wheeler and Simpson (2019)

perspective, 5G could result in a bigger and more attractive target for hostile agents. On the other hand, 5G offers significant improvements over 4G networks on key security aspects such as user authentication and data encryption. Examples include trusted non-3GPP access, security aspects for small data mode, user plane DoS attacks, security mechanism differentiation for network slices, relay security and Broadcast/Multicast security, and capabilities to deal with rogue base stations.[94]

Other potential adverse effects may result from disaggregation, such as bottlenecks and lock-in to new types of dominant suppliers. On the one hand, some respondents believe that a multi-vendor environment where suppliers provide different hardware could potentially lead to added cybersecurity risks. According to this view, Open RAN brings a trade-off: while it can bring more interoperability, it may also exacerbate cybersecurity risks. This is because the opening of interfaces will provide more entry or attacking points for hackers, irrespective of which vendor provides the hardware and which country this vendor comes from. Most hacking instances happen at the terminal side because hackers look for weak points they know well. As a result, an opening of interfaces will make the system more known by hackers; and hackers may find it easier to have the necessary skills to penetrate these networks. Moreover, the security environment of network components provided by different vendors varies, which brings the risk that certain elements cannot ensure the system level of security. Therefore, there may be a need to ensure that all vendors that come into the market have the capabilities to fulfil security requirements, which are different for the telecommunications and internet industries; in telecommunications, fulfilling cybersecurity requirements currently requires companies to invest heavily in hardware and software. Finally, there is a question about which actor will acknowledge responsibility for a failure or bad performance in an identified point of the supply chain.

On the other hand, others argue that an open environment can make these risks more controllable, and transparency can make it easier to know where problems are and therefore how to solve them. According to this view, higher flexibility can make it is easier to find parties that deploy new software updates to solve security vulnerabilities when identified (assuming a proper architecture and cybersecurity capabilities). However, it may be necessary to perform more security checks as Open RAN brings a more complex environment than an integrated solution from a proprietary vendor.

When assessing the security implications of Open RAN, one interviewee observed that Open RAN is primarily about technically evolving RAN to becoming virtual, more software-based, cloud-based RAN. Although Open RAN will lead to disaggregation of components in the RAN, such a shift to cloud-based RAN carries inherent security risks. These risks could be in the integration of Open RAN with 3GPP RAN, risks that are inherent to any virtual RAN, cloud environments including vulnerabilities in open-source software, and third-party hardware. Since Open RAN will attract new market entrants aiming to unseat the incumbent network equipment providers, there are also potential risks as they scale up their capabilities in terms of security, hardening of hardware, and processes for vulnerability disclosure and distribution of patches.

An interviewee argued that current regulation and legislation around 5G in Europe is currently light-touch and that such guidance means that important decisions often have to be retrospectively pieced together through case law when organizations end up in court. The European Commission could help by providing more detailed and specific guidance around what is a complex and highly technical area to help actors in this space make well-informed proactive decisions. Continuously requiring software producers to implement individual security solutions that are built into their applications could provide an additional layer of security.[95]

94 For more details see Ahmad et al (2017, 2018); Zhang et al (2017)
95 Tăbușcă and Tăbușcă (2019)

The 2019 Cybersecurity Act established the European Cybersecurity Certification Framework, which enables the EU to create market-driven EU-wide certification schemes to reduce fragmentation between existing cyber certification schemes.[96] To this end, the European Union Agency for Cybersecurity (ENISA) is launching a certification framework on 5G which aims to enhance security and patch vulnerabilities while addressing certain risks and concerns about third-country operators as part of a risk mitigation strategy.[97] - 3GPP is the main body developing technical specifications for 5G networks, including security specifications. However, some of these security controls are regarded as optional or there is a degree of flexibility left to suppliers on how to implement and for operators on how to interpret and utilize the control.[98]

Scenario-specific assessment

Experts differ in their assessment on the extent to which cybersecurity held critical implications for the scenarios. This section also provides a summary of potential opportunities and threats concerning cybersecurity for MNOs, vendors, and the 5G ecosystem as a whole.

Scenario I: Incumbent players driving 5G

In this scenario, MNOs and incumbent network equipment providers will likely remain the main actors and drive 5G if the capabilities and coverage of 5G are not expanded quickly, as this may provide them with additional time to adapt to changes in the market.

However, incumbent telecommunications operators may need regulatory supervision and may need to invest in their cybersecurity capabilities, as this is one aspect where new actors in the market may have a comparative advantage. New players in this space are typically not hampered by legacy technologies, or by legacy business models that some of the existing telco operators have; incumbent operators have a business model and established architecture that has been honed over 25 years to serve end-users. With an existing end-user base, incumbent telco operators may be well-placed to connect these devices and their users using 5G.

Vendors are participants in several existing Open RAN initiatives and can position themselves to adapt to changing industry demands if needed. However, this still risks a lack of diversity in 5G players that may create path dependency and weaken the resilience of networks.

Scenario II: Slow pace of 5G Roll-Out

The slow roll-out of 5G may have an impact on cybersecurity because it could give operators and equipment providers a different latitude to weigh the risks and address them before the risks are more widespread. On the other hand, limited risk of exposure also increases the probability of cybersecurity risks remaining undetected for longer durations. The commercial imperatives to address cybersecurity risks in 5G equipment which is not in widespread deployment and therefore affects limited end-user segments are difficult to ascertain and will differ for operators.

Subject to the procurement and deployment strategy followed by the operators and their chosen vendors, this scenario also raises the possibility that the firmware or the software on the equipment is of date or not correctly patched due to a lengthy gap between procurement and deployment. In case the cybersecurity risks prove to be vendor-specific, the slow roll-out scenario could also present an opportunity for operators to revise their vendor selection strategy or create a differentiated strategy based on regional considerations, and requirements of core/access network deployments.

In the context of vendors relying on Open RAN solutions, slow 5G roll-out also presents a potential opportunity to establish the business case (including demonstrable ROI) for their solutions over established vendors. However, the slow 5G rollout could also mean longer time delays for any

96 European Union (2019)
97 ENISA (2021a)
98 ENISA (2021b)

potential Open RAN deployments, making it more challenging for Open RAN solution providers to demonstrate their business case.

Scenario III: Open RAN as a game-changer

While this scenario can bring higher degrees of interoperability, it can also exacerbate cybersecurity risks. For the Open RAN as a game-changer scenario, there may be a higher cybersecurity risk because the opening of interfaces will provide more entry or attacking points for hackers, irrespective of which vendor provides the hardware and which country this vendor comes from. Most hacking instances happen at the terminal side because hackers look for weak points they know well. An opening of interfaces will make the system more known by hackers, and hackers may find it easier to penetrate these more open networks. Open RAN initiatives such as O-RAN Alliance acknowledge this issue and have set up working groups to address this.[99] Other potential challenges that may not be solved in this scenario are the movement from hardware-focus to software-focus, the increase in attack surface, and the use of machine learning.

Scenario IV: 5G for Big Tech

This scenario presents both challenges and opportunities in terms of cybersecurity. On the one hand, Big Tech have well-established protocols in place to identify and publish resolutions for cybersecurity risks for their existing software/hardware platforms and are well-versed with scaling mitigation measures for potential cybersecurity risks. On the other hand, however, Big Tech lack the experience of traditional equipment vendors in addressing cybersecurity risks in communications networks in liaison with operators (i.e. external stakeholders).[100] Even if the risks are software-based or contained in cloud-based RAN deployments, Big Tech would need to develop sufficient expertise and experience to manage the relevant path dependencies in coordination with other stakeholders (including primarily the operators). The challenges that are considered to be inherent to 5G technology, such as around virtualization and the increase in attack surface, may not be solved through this scenario.

99 More information about these working groups can be found at: https://www.o-ran.org/blog/2020/10/24/the-o-ran-alliance-security-task-group-tackles-security-challenges-on-all-o-ran-interfaces-and-components

100 An example in a different platform provider-operator-hardware provider ecosystem is that of the Android smartphone ecosystem. The updates to Android operating system rely on coordinated action from Google (the company developing the operating system), smartphone manufacturers and wireless service providers. Evidence suggests that the security updates are not always delivered to the end-users on time due to differing commercial, technical priorities on part of the various stakeholders. See Farhang, S., Laszka, A. and Grossklags, J., 2018, February. An economic study of the effect of android platform fragmentation on security updates. In International Conference on Financial Cryptography and Data Security (pp. 119-137). Springer, Berlin, Heidelberg.

h. Energy efficiency and consumption

Current situation and sources of impact

There are a variety of areas to consider in looking at the energy efficiency of 5G. This includes the energy efficiency at base stations, the efficiency of caching, energy-efficient non-orthogonal multiple access (NOMA), and energy-efficient resource sharing (see Figure 5).

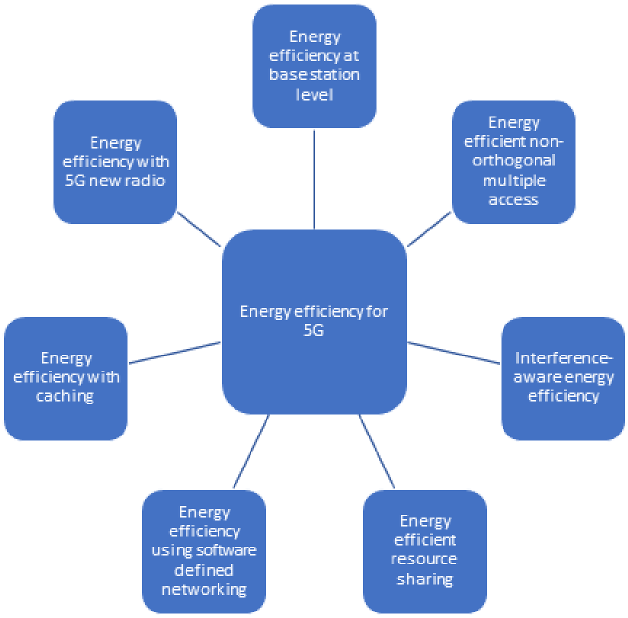


Figure 5: Different areas of energy efficiency for 5G[101]

There may be scope for optimisation at each of these levels. For instance, the energy efficiency at the base station level could potentially be optimised by functional split architecture for the 5G backhaul,[102] and there may be scope for improved energy efficiency using software-defined networking such as separated control and data planes in a heterogeneous network.[103] Some experts expect improvements in energy efficiency in 5G as it has built-in functionality for greater energy efficiency compared to 4G, such as the sleep/idle time between transmission. However, this may be outweighed by the larger number of antennas, particular in the case of Open RAN architectures. In addition, the increase in data volume enabled by 5G, ultimately leading to an increase in total energy consumption, has to be taken into account as well.

Impact of Open RAN and other trends

4As noted in the release of the specification of 3GPP, energy-saving measures introduced to achieve a better energy efficiency performance include the removal of always-on reference signals, enlarged broadcasting synchronization signal intervals, and base station sleeping mechanisms in light load conditions.[104] Another proposed feature is cell zooming – which adjusts the cell size based on traffic load. In addition, various approaches have been proposed to improve the spectrum efficiency (which may be defined as the ratio of data rate to bandwidth) – such as massive multiple-input multiple-output (MIMO), Non-Orthogonal Multiple Access (NOMA), and advanced coding and modulation.[105] The standardisation work on NOMA schemes is ongoing and could expand the achievable network

101 Based on Usama and Erol-Kantarci (2019).
102 Nawawy et al. (2018)
103 Klapez et al. (2018)
104 Nawawy et al. (2018)
105 Larsson et al. (2014); Ding et al. (2017); Niu et al. (2014)

capacity, also known as the sum capacity, by having multiple users scheduled on the same time or frequency resource in downlink or uplink.[106] In waveform overlapping multiplexing (WOM) schemes, traditional single-input single-output (SISO) systems can be transformed into MIMO systems, in which a waveform is analogous to an additional antenna.

Open RAN is likely to open up non-real-time and real-time RAN Intelligent Controller aspects of the infrastructure, in which AI and data collection tools can work out best practices and optimize systems. However, it remains to be seen whether the positive optimizations gained through AI power management will more than offset any limitations on the hardware side from the fact that the components might not be using the best power management chipsets or internal design. One interviewee highlighted that Open RAN solutions only support 4G and 5G networks so even if operators are to switch to Open RAN for 4G and 5G entirely (an unlikely scenario soon), this does not resolve the need to run 2G and 3G networks on incumbent network equipment stacks. This may result in increased energy consumption for the operators due to the need to run an integrated network.

The role of chipsets in achieving energy efficiency in potential 5G and Open RAN deployments is likely to be an important factor. One interviewee suggested that the next generation of chipsets produced by a vendor such as Qualcomm are likely to challenge incumbents such as Ericsson, Nokia, and Samsung on parameters such as power consumption and CO2 emissions. Purpose-built chips work better at present in terms of integration. The next generation of chips might enable Open RAN to deliver better performance in terms of power consumption. However, as the Open RAN equipment vendor ecosystem continues to evolve and Open RAN equipment providers continue to make gains in terms of power consumption (including AI-enabled real-time power management as highlighted above), components in existing single-vendor ecosystems will also draw on such technological improvements to a great degree. Incumbent players argue that there is a strong difference between specialized hardware (i.e. customized ASICS) and off-the-shelf hardware and the difference is expected to be three to four times on average in terms of power consumption.[107] Components in single-vendor solutions are designed and optimised for specific functions and seamlessly integrated with other components. As there are fewer interfaces, there is more freedom to move functionality and increase integration and performance and therefore reduce energy consumption. In contrast, in Open RAN the space for optimisation is reduced as components serve more discrete functions. Equipment designed based on Open RAN specifications currently does not allow unique enhancements on the fronthaul interface for the customer.

Therefore, whether Open RAN will deliver any advantages over solutions delivered by incumbent providers remains to be seen. In case Open RAN specifications deliver better power consumption outcomes, incumbent network equipment providers could also adopt Open RAN solutions in their equipment. In such a case, Open RAN could help entrench the market positions of the incumbent network equipment providers further in conjunction with their existing network equipment products and services portfolio.

Several interviewees highlighted the strengths of existing incumbent ecosystems in terms of their capabilities to deliver interoperable, highly scalable, secure, and standards-compliant equipment albeit as part of proprietary solutions. There are currently a limited number of Open RAN deployments in practice (for example Rakuten in Japan, and Drillisch in Germany, and a few pilot deployments including by Vodafone and Telefonica). Available datasets for energy consumption of Open RAN solutions for 5G indicate that Open RAN solutions are likely to be less energy efficient than the RAN solutions (including cloud RAN) provided by incumbent equipment providers.[108]

106 Ding et al. (2017); Chih-Lin et al. (2020)
107 Incumbent players also argue that the increased use of ASICS for some products (e.g. electric cars, laptops) for the purpose of power consumption is in the opposite direction advocated by Open RAN and its strategy to use COTS, so one argument.
108 Patrick et al. (2021)

While improvements in energy efficiency may reduce the cost of kWh per GB of data, the total volume of data through the 5G network will grow – meaning that the total energy consumption will increase. The market for human consumer devices connected to the network is close to saturation point but the overall number of connected devices is expected to grow to 100 billion by 2030 as the IoT adoption grows.[109] In addition, the 5G network will require more antennas, larger bandwidths, and a higher density of base stations.[110] This observation was also echoed by one interviewee who highlighted that any current assessments on energy consumption are dependent on the actual data transfer that takes place when 5G networks and Open RAN solutions for 5G are widely deployed.

An additional challenge concerning the energy efficiency of 5G networks relates to the cooling systems at base stations. Cooling systems account for 24% of total power consumption.[111] However, the energy consumption of base station cooling systems can be significantly reduced if a Cloud-RAN architecture is utilized[112], through passive cooling using CPU heatsinks[113], or through liquid cooling – which could reduce expenses at base stations by 30% and emissions by 80%.[114] Where the annual energy consumption of an air-cooling system is 3190 kWh, the liquid cooling annual energy consumption is 800 kWh.[115]

Energy efficiency, defined as the ratio of the data rate to total consumed power, is a key performance indicator of 5G.[116] Given the expected growth of traffic, an improvement in energy efficiency is important. Otherwise, with 5G the power consumption will rise considerably with a negative impact on the CO2 emission, too. Yet, standardized data about the efficiency of vendors and operators either do not currently exist or are difficult to find. To improve energy efficiency in the 5G equipment standards and consistent data across vendors and operators need to be available.

As the discussion in the Cost dimension (section 3.3) highlights, energy efficiency is only a component of the overall cost of a 5G network. Costs of system integration, long-term maintenance requirements of networks, the site at which the RAN solutions are deployed (whether greenfield or brownfield), and whether the RAN (Open or proprietary) deployments are Cloud-based are equally important (and yet highly variable) components of the cost assessment (amongst others). Based on current developments in Open RAN specifications whether Open RAN solutions will match the energy efficiency of traditional proprietary RAN solutions remains to be seen. Should Open RAN solutions match or supersede the energy efficiency of proprietary RAN solutions, this may not necessarily translate into Open RAN solutions delivering cost savings to network operators. To make any definitive assessments on the advantages or drawbacks of Open RAN vs. proprietary RAN solutions, longitudinal datasets on the energy performance of these solutions need to be collected in similar market conditions to conduct further robust cost/benefit analyses vis-a-vis energy efficiency.

Scenario-specific assessment

In terms of energy efficiency, interviewees differed about the potential of Open RAN, the role of Open RAN for Big Tech, and the extent to which Open RAN could be considered a viable long-term solution if the focus was on 5G networks optimised for energy consumption. This section also provides a summary of potential opportunities and threats concerning energy efficiency for MNOs, vendors, and the 5G ecosystem as a whole.

Scenario I: Incumbent players driving 5G

In this scenario, interviewees highlighted that incumbent telco operators are likely to draw on their existing extensive experience of running network resources at optimal capacity and effective network

109 GeSI (2015)
110 Chih-Lin et al. (2020)
111 Mughees et al. (2020)
112 Checko et al. (2015)
113 Asian et al. (2019)
114 O'Halloran, (2020); Huttunen et al., (2020)
115 Huttunen et al. (2020)
116 Chih-Lin et al. (2020)

resource allocation strategies according to end-user demands at peak and off-peak times. As a result, such a scenario may prove beneficial from an energy efficiency perspective. However, energy efficiency implications in such a scenario would depend on operator strategy for inventory management, their decision to expand the selection of vendor pool for RAN deployment (including in-house and external Open RAN solutions), and the operators' system integration strategy for Open RAN and proprietary 5G equipment. Faced with the risk of becoming bandwidth pipes to content providers (such as Netflix or Amazon Prime) telco operators are expanding their services footprint to become systems integrators and reference design providers, and are developing content platforms of their own. Notable examples mentioned by interviewees included Rakuten (Japan), Jio (India), AT&T (USA), Telefonica (Spain/Europe), Vodafone (UK/Europe), Deutsche Telekom (Germany/Europe), and NTT (Japan). Such operators are likely to be in an advantageous position in the scenario where incumbent players are the main drivers of 5G deployment. Collecting standardised data on base station power usage could provide opportunities to improve energy efficiency and reduce costs for incumbent players. Nokia has reported that liquid cooling base stations could reduce emissions by 80%.[117]

Scenario II: Slow pace of 5G Roll-Out

In a slow roll-out of the 5G scenario, operators may rely on existing networks – where there is a sunk cost in terms of manufacturing and carbon footprint. This may delay increased data usage and energy consumption which is likely in the case of a ubiquitous 5G network availability. Although existing 2G/3G/4G networks have inefficiencies, the experts suggest that slow 5G roll-out could prove unintentionally beneficial in terms of also delaying the increased data and energy consumption due to 5G networks. Such a scenario could allow more time for improvements in AI-based power management techniques to be integrated into chipsets, for example. However, if these improvements are directly tied to procurement or deployment cycles of 5G networks, the improvements in AI-based power management techniques may also develop at a slow pace. This may delay optimisations in areas such as resource sharing, non-orthogonal multiple access and caching. Such a scenario could also delay the adoption of RAN equipment provided by incumbent network equipment providers. The slow pace of the 5G roll-out scenario could prove beneficial to Open RAN as it could provide more time for Open RAN solutions to improve and to potentially achieve energy performance levels similar to the RAN solutions delivered by incumbent network equipment providers. However, it could also slow down the potential adoption of Open RAN-based equipment by operators. The slow pace of 5G roll-out scenario could also delay improvements in Open RAN specifications, the activities of the Open RAN working groups (particularly those tasked with performance management, including energy consumption-related performance) as the commercial imperatives of the industry participants may not always align the objectives of the Open RAN technical specifications being developed.

Scenario III: Open RAN as a change-maker

Based on available evidence, interviewees suggested that Open RAN as a change marker scenario may prove to be the least efficient outcome in terms of energy performance of 5G networks. Open RAN specifications are still evolving and are focused on open interfaces at this stage. Their long-term reliability is not known. Based on the current development of Open RAN, it is difficult to measure and control energy in each part of the network, and there is less centralized oversight of overall energy consumption. In the case of this scenario, this lack of centralized oversight on energy performance could increase operator costs as they adapt to the needs of increased system integration with Open RAN equipment, integration with existing 2G/3G/4G equipment, and higher complexity of end-to-end performance management. Based on existing Open RAN energy performance metrics, when considered in conjunction with potential cloud RAN solutions based on

117 O'Halloran (2020)

Open RAN and the need to integrate any in-house Open RAN solutions, energy efficiency is likely to be the weakest in the Open RAN as a change marker scenario according to the experts.

Scenario IV: 5G for Big Tech

Some experts indicate that in the event of a 5G for Big Tech scenario, tech companies could be well-placed to draw on their existing, extensive experience of managing large, decentralised, distributed data and server infrastructure. Since Big Tech companies also have significant in-house AI capabilities such a scenario also presents opportunities for AI-based power management techniques in their RAN equipment offerings (including those based on Open RAN). Big Tech companies with experience in running large decentralised networks such as Microsoft, Amazon and Google may become important market players in such a scenario. In addition, interviewees suggested that 'tech' companies such as Intel, Qualcomm, Arm, NEC, Samsung, Dell, IBM, HPE, Oracle, SAP, and potentially Baidu, Alibaba could also become relevant players in the provision of 5G network equipment and deployment in this scenario. Since 5G is designed to be 'cloudified' and virtualised, tech companies specialising in the provision of cloud services and infrastructure could also play a key role in this scenario. Given Big Tech's strengths in managing cloud platforms, such a scenario could present an opportunity for growth in CloudRAN solutions based on either Open RAN or proprietary solutions. However, whether the increased use of Cloud RAN based on Open RAN would result in energy efficiencies is not clear given the current energy performance metrics of Open RAN. Experts also highlight that Big Tech face a steep learning curve in delivering high energy efficient RAN equipment given their lack of expertise in understanding variations in network utilisation across different regions and operators' strategies for managing demand for network resources. In addition, ongoing anti-trust investigations about the role of Big Tech's market goalkeeper roles and their perceived dominance in cloud services indicate that there is uncertainty about whether Big Tech would enter a heavily regulated market space with well-established incumbent network equipment providers. There are also potential challenges in such a scenario as climate change mitigation strategies such as carbon taxes may increase operating costs for Big Tech.

i. Interoperability: standards needs and licensing issues

Current situation and sources of impact

Widely accepted standards are the core element of successful telecommunication networks because they allow the development of positive network externalities, i.e. bilateral connections between the users. Due to the transition from fixed to mobile telephony, various mobile networks could be developed in parallel based on different and even incompatible technologies. The competition between different technologies was the approach in the US, whereas in the EU the decision was already taken in an early stage for the GSM technology, which turned out - from a technological perspective - not to be the most superior solution.[118] However, the timely decision for a common mobile communication standard in Europe is a success-case of European standardisation in general[119], but in particular both for the European mobile network operators (MNOs) and the European vendors, like Nokia and Ericsson.

However, we observe also that the influence of European technology providers is shrinking in the last decades. In particular Asian and lately Chinese companies have not only caught up to the European and US companies from the second over the third to the fourth generation of mobile communication standards based on the declaration of so-called standard-essential patents.[120] Recently, they have even taken over the leading position not only based on the declaration of standard-essential patents (SEPs) but also taking the massive contributions to the specifications of

118 Cabral & Salant (2014)
119 Pelkmans (2001)
120 Von Laer, Blind & Ramel (2021)

5G into account.[121] Here, the Chinese state-owned company Huawei, but also ZTE have to be explicitly mentioned. However, the European players, Nokia and Ericsson can at least keep their shares in this fierce technological competition due to heavy R&D investments.

The standardisation activities related to 5G are taking place within the 3rd Generation Partnership Project (3GPP), which is supported by seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC). The 3GPP headquarters is located at ETSI. ITU was originally the institution being responsible for standardisation in telecommunication driven by the formerly state-owned telecommunication operators. However, ETSI was after its foundation in 1988 able to take over a leading position due to the increasing importance of information and communication technologies and recently the Internet, but also due to its successful positioning as an international hub for standardisation.

Whereas standardisation in general, but also standardisation in mobile communication has originally been focusing on hardware, the role of software-based solutions and virtualization has been only recently dramatically increasing. The increasing role of software has been expressed by Andreessen (2011) ten years ago with his article on “Why Software Is Eating The World”.[122] However, we do not only see an increasing role of software, but also open-source software expressed by Biddle (2019) two years ago with his article on the Linux Foundation eating the world.[123]

While historically standardisation bodies focused on hardware interoperability, open-source software is increasingly part of how interoperability occurs. Consequently, standardisation bodies and processes are also increasingly confronted with open-source software as possible input into their processes, but also as an option to implement their standards. Furthermore, open-source foundations are starting to claim not only to organize the development of open-source code but also to release standards based on open-source code.[124]

Consequently, we have new organisations in the standardisation landscape, labelled as young technology specialists in the context of a taxonomy of 100 consortia in the field of mobile telecommunications published by Teubner et al. (2021).[125] Without naming the Open RAN Alliance, they have identified many open-source organizations denoted by young technology specialists, which do not formally interact with 3GPP. However, they observe that their technologies can still serve both as an add-on or in competition to 3GPP.

The O-RAN Alliance is the key player for the further specification to enable an open, interoperable 5G supply chain. According to the O-RAN Alliance, the O-RAN architecture is based on standardized interfaces to enable an open, interoperable ecosystem in full support of and complementary to standards promoted by 3GPP and other industry standards organizations[126]. Also in the Memorandum of Understanding (MoU) on the “Implementation of Open RAN based Networks in Europe” signed in January 2021 by several European MNOs, they commit themselves to support the continued development and recognition of Open RAN specification and standards through O-RAN Alliance and other standard-setting organizations to enable a true multi-vendor environment. One MNO representative states that O-RAN is complementing the 3GPP radio standard by making valuable contributions to open architectures, providing a relevant set of reference architecture specifications and the interfaces that connect its components, fundamental for the development of open solutions based on connectable components. Representatives of vendors do not perceive O-RAN in competition with 3GPP, but more being responsible for the implementation of open-source-

121 Pohlmann, Blind & Heß (2020)
122 Andreessen, M. (2011, August 20). Why Software Is Eating the World. The Wall Street Journal. Retrieved from https://www.wsj.com/articles/SB10001424053111903480904576512250915629460
123 Biddle &Bradford (2019)
124 See Blind & Böhm (2019) for a first comprehensive study on the interaction between standardisation and open-source software.
125 Teubner, Henkel & Bekkers, (2021)
126 O-RAN Alliance White Paper, “O-RAN: Towards an Open and Smart RAN,” https://www.o-ran.org/resources, 2018.

based standards or specifications. The governance of the O-RAN Alliance is briefly described in the mentioned MoU. However, the section on the governance provides no indication, whether it complies with the six principles for the development of international standards, guides and recommendations to ensure transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and to address the concerns of developing countries.[127]

In detail, based on publicly available information[128] and an interview with a legal expert of the WTO rules also applicable according to EU Regulation No 1025/2012, the following conclusions are derived:

- First, the required transparency, i.e. all essential information is easily accessible to all interested parties, is only partly fulfilled, e.g. the O-RAN specifications are not accessible at the homepage.
- Second, the procedure is not open in a non-discriminatory manner during all stages of the standard-setting process, because the founding members have access to more information than the contributors during the process.
- Third, although interested contributors have opportunities to contribute to the elaboration of the specifications, the founding members have a privilege, because they have the necessary minority of more than 25% to block proposals.

Overall, proof that the O-RAN Alliance complies with the various WTO criteria is still missing, although some of their members assure this compliance. Consequently, such an independent assessment is needed, which, however, cannot be realised within the context of this project.

The role of interoperability in general and standardisation in detail related to 5G and Open RAN have only lately addressed by very few academic papers.[129] Bonati et al. (2020) remark that researchers and an increasing number of standardisation bodies and industry consortia have recognized softwarization, virtualization, and disaggregation of networking functionalities as the key enablers towards more flexibility. In particular, software-based cellular networks are perceived as the technological solution to satisfy the new dynamic and application-driven traffic requirements, because their openness through well-defined interfaces and programmability allows swift and responsive network optimization. Several 5G software-based projects and alliances, including the O-RAN Alliance, have integrated an open-source approach.

According to statements by interviewees and the presentation of the O-RAN Alliance to the public, the Alliance can be considered as an industry consortium mainly driven by MNOs.[130] The O-RAN Alliance tries to re-shape the RAN industry towards more intelligent, open, virtualised and fully interoperable mobile networks[131]. O-RAN based mobile networks try at the same time to improve the efficiency of RAN deployments as well as operations by MNOs.

To achieve these goals, O-RAN Alliance is active in three main streams:

- The specification effort => new standards for open and intelligent RAN
- O-RAN Software Community => open software development for the RAN (in cooperation with the Linux Foundation)
- Testing and integration effort => supporting O-RAN member companies in testing and integration of their O-RAN implementations

The ORAN Alliance is promoting the definition of an open standard for the vRAN, with just two goals[132]. The first is the integration of machine learning and artificial intelligence techniques in the RAN. The second is the definition of an agile and open architecture, enabled by well-defined

127 https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm
128 https://www.o-ran.org/membership-info
129 See for example Bonati et al. (2020)
130 https://www.o-ran.org/about
131 See O-RAN Alliance Mission Statement
132 Bonati et al. (2020)

interfaces between the different elements of the RAN. Since all O-RAN components must have the same APIs, it is in theory possible to substitute single components. In principle, this allows O-RAN-based 5G deployments to integrate components from multiple vendors and thus to open the RAN market to third party entities providing new functionalities and diversified services. In theory, the open interfaces allow to adapt flexibly COTS hardware and consequently to reduce costs. Eventually, following the trend started with cloud-native infrastructures, the O-RAN Alliance also aims at promoting open-source software as part of the consortium effort.

Regarding standardisation, O-RAN aims to standardise the interfaces between the components of the whole architecture. In addition, the interface related to operation and management functions tries to be compatible with existing standards to permit seamless integration with existing management frameworks, like the IETF Network Configuration Protocol and several 3GPP-defined APIs or specifications.

Besides standardisation activities, the O-RAN Alliance has established a software community in collaboration with the Linux Foundation for contributing Open-source 5G software that is compliant with the O-RAN specifications. The O-RAN Open-source software tries to enable 5G networking in a standardized environment.

According to Bonati et al. (2020) and several interviewees both from MNOs and vendors, Open RAN is not at the production level yet. Therefore, future releases of their specifications are needed to complete the integration of the different RAN components. Although operators, vendors and scientists are paying considerable attention to O-RAN Alliance, its specifications are not yet ready for being implemented in commercial 5G networks. They identify the following barriers:

Competition with standardisation

There is constant pressure to keep up with the specifications/technologies being introduced by new communication, networking and even programming standards. In addition, the testing of real-world 5G software is extremely complex due to the lack of accessible open hardware for the software to run. Bonati et al. (2020) suggest a more concerted, joint software development effort, also in hardware platforms that can keep up with the requirements of the software community.

The O-RAN standards do complement the RAN standards set by 3GPP. But O-RAN specifications are not yet endorsed and available as ETSI standards specifications, which would be beneficial for even further adoption. However, a first collaboration agreement has been signed in April 2021, which, however, focuses mainly on IPR policies. Consequently, licensing is not affected because both 3GPP and O-RAN licensing schemes are based on FRAND. However, the majority of patents are declared to standards released by 3GPP at ETSI, whereas the declarations to the O-RAN Alliance are not known.

Limited contributions to O-RAN open-source software

The same large telecom operators and vendors driving the development of open-source frameworks are not investing the same effort to O-RAN related projects. Here, representatives of academia or from smaller companies are more active but with limited manpower and resources. As some digital signal processing and implementations of the lower layers of the RAN stack are often protected by patents and are therefore generating product-bearing revenues, major vendors and MNOs are not encouraged to release their solutions as Open-source. Consequently, the OpenAirInterface (OAI) Software Alliance has licensed the OAI RAN implementation with a permissive license, which allows contributors to retain intellectual property claims. Additionally, the O-RAN Alliance is encouraging an openly software-based RAN. However, the current development efforts do not include also an open-source software for the radio front-ends. Therefore, the wireless community has to increase its support toward the development of complete and Open RAN and radio software libraries, increasing the number of active contributors to the currently available open-source RAN projects.

Lack of robust, deployable, and well-documented software

According to Bonati et al. (2020) and several interviewees, most of the frameworks and libraries provided by O-RAN cannot be used in actual networks, as their open-source component is either incomplete, requires additional integration and development for actual deployment, or lacks robustness. Moreover, to reach the quality of commercial solutions, the open-source community has to deliver well-documented, easy-to-deploy, and robust software, specifying all dependencies and additional software components that guarantee the correct and efficient functioning of the system.

Missing testing and certification environment

In addition to the obstacles identified by Bonati et al. (2020), MNOs perceive it as the next challenge for O-RAN to provide the right environment to test, verify compliance and certify O-RAN-based products. One example of a testbed to check also interoperability issues is SONIC, which has been recently launched.[133]

To conclude, all these barriers are preventing, or considerably slowing down, the widespread and frictionless application of several of the O-RAN solutions.

Scenario-specific assessment

In the following section, we assess the role of interoperability and standardisation incl. licensing issues based on the expert interviews.

Scenario I: Incumbent players driving 5G

There are some specific opportunities and threats for MNOs. MNO opportunities exist by enlarging the supplier base and increased competition, thus reducing the dependency on few remaining suppliers. This is finally only successful by really open (non-proprietary) interfaces and is seen as a key enabler for MNOs to stay competitive. In addition, MNOs hope to benefit from an increased resilience, programmability and flexibility of their networks as well as from new innovative features and applications which can be built on top of an open and virtualized network architecture.

The threat to the MNOs is caused by too little acceptance of O-RAN standards and specifications by the incumbent players because the reciprocal acceptance of standards between 3GPP and the O-RAN Alliance has not been agreed upon. On the one hand, the market fragmentation might increase, which eventually hinders more vendor diversity. On the other hand, interoperability is becoming more crucial for MNOs if more different suppliers enter the markets. In addition, the delaying take-up of O-RAN and the parallel trend towards cloudification will strengthen the role of the cloud players building few RAN solution silos and further pushing out European RAN players.

Vendors make strong contributions to standardisation both at 3GPP for decades, but also meanwhile to the O-RAN Alliance. Due to their long-lasting history of making intensive contributions to standardisation, they will have also an important role in future standard-setting both at 3GPP, but also at the O-RAN Alliance. Despite the increasing competition in specific components due to more standardisation efforts in the O-RAN Alliance, which allow the market entry of new players. Big vendors might turn in the role of system integrators, which become more important if more specific components are supplied by a diverse and increasing group of small suppliers.

Concerning the threats, interoperability is more crucial for small vendors, in particular entering the market, because they have to find the niche for their technologies and products. And these entrants will have in general not the capacities and experience to influence standardisation.

On the ecosystem level, the EU is challenged by the effort in particular of Chinese companies related to standardisation both at 3GPP and the O-RAN Alliance. Therefore, incumbent EU players are

133 https://uk5g.org/discover/testbeds-and-trials/sonic/

challenged. There is still enough time for EU vendors - both existing and new - to enter the market and fill current gaps, but more action and commitment is needed as well as political support.

Scenario II: Slow pace of 5G Roll-Out

This scenario is mainly focused on the low speed of the roll-out of 5G in some countries due to regulatory hurdles and limited investment. However, it is based on already existing 3GPP standards and Open RAN specifications. Therefore, there is no major impact on further standardisation or interoperability as such. However, the existing O-RAN specifications are not yet able to address the increasing cybersecurity problem within this scenario.

In general, the slow 5G roll-out has eventually negative implications for standardisation both at 3GPP and ORAN Alliance, because the delayed deployment will also lead to less feedback from the applications of 5G standards in practice back to standardisation.[134]

Overall, this scenario is threatening both the MNOs and vendors in the EU, i.e. also the whole ecosystem in the EU, because the competitiveness of the European players will be reduced, which eventually weakens also their position in standardisation.

Scenario III: Open RAN as game-changer

In case of an O-RAN triumph, the consequence would be, that the O-RAN architecture and its specifications would become (de facto) standards for RAN. When the O-RAN Alliance is complying with the WTO criteria and EU Regulation 1025/12, O-RAN standards would be endorsed and available as ETSI standards, which is not yet the case. This adoption would be beneficial for even further adoption of the O-RAN architecture.

MNOs face some specific opportunities and threats. The MoU by several European MNOs documents very well the opportunities the MNOs expect from this scenario also related to standardisation. The O-RAN architecture will attract new suppliers of components, which might eventually also contribute to standardisation both at 3GPP and the O-RAN Alliance. The increased diversity and competition between suppliers will benefit the MNOs.

The new capabilities under this scenario also driven by the greater variety of vendors will enable new use cases and services benefitting customers and European society as a whole.

Concerning the threats for MNOs, patent laws in several European countries where injunctive relief is much stronger than in the USA and Asia could disadvantage O-RAN rollout in Europe despite the application of FRAND licensing also by the O-RAN Alliance, like by 3GPP at ETSI. In addition, if the O-RAN architecture is implemented as a proprietary solution, then there will be limited positive feedback into the standardisation processes. Moreover, one can assume, that if the security issues are not solved, the roll-out of O-RAN architecture and specifications is challenged.

This scenario can be also very attractive for vendors despite the expected increasing competition due to new entrants, which in particular is beneficial if open standards and specifications lower the barriers to entry. The incumbents can benefit from the contributions of the new entrants, incl. from open-source communities to standardisation increasing the quality and eventually the acceptance and deployment of standards and specifications. Eventually, well-defined standards between the increasing number of components and applications open new opportunities for system integrators, which can be either the incumbents, but also new players.

Under this scenario, interoperability and therefore standards will become more relevant in general, but in particular for small players to find and establish their niche markets. The incumbents can still exploit their strong position also in standardisation for pursuing their interests.

134 Blind & Gauch (2009)

The new small players face not only the challenge to deal with the complex landscape of intellectual property rights, i.e. standard-essential patents.[135] In complex products with many components provided by different vendors, the liability of the whole product has to be clarified, because small players have not the knowledge and resources to deal with this risk. Consequently, the incumbents have an additional strategic advantage.

Standards generated under this scenario can still be used by governments to establish protectionist trading policies.

On the 5G Ecosystem level, some opportunities and threats can be discussed as well. According to the MoU, the O-RAN Alliance supports the development and recognition of O-RAN specifications also at standard-setting organizations to enable a true multi-vendor environment. The support of standard-setting organizations aims to resolve missing concepts and specifications in the area of management, orchestration and operation of Open RAN, as required, e.g. to support the O-Cloud model. Overall, the MoU supports the unification of the concept of Open RAN technology around the industry-approved O-RAN architecture to avoid ambiguity in the industry and to provide related guidance for the rollout of Open RAN.

If the standardisation activities and results of O-RAN and alike organizations are open, coordinated and accessible for all interested stakeholders, e.g. by acceptance of O-RAN specifications as 3GPP standards, the whole ecosystem will benefit. Consequently, a competitive European Open RAN ecosystem of technology providers and system integrators, thus strengthening and expanding the European RAN industry will be possible.

There are also some threats in this scenario for the 5G ecosystem. Due to an increasing number of stakeholders in standardisation also from outside Europe and from open-source communities, the efforts to achieve interoperability and standards are going to increase. The time to find a consensus might also be extended. Solving (cyber-)security issues might become more complex, also due to the increasing role of open-source software, which might challenge in particular MNOs, the O-RAN Alliance, but also 3GPP.

Not only the number of actors involved in standardisation might increase, but also new institutions might emerge, similar to the rather young O-RAN Alliance. If there is a lack of coordination of standardisation work and output (also related to quality and performance), the interoperability and eventually the performance of the whole system will be challenged. In particular, different and sometimes competing standardisation cultures and approaches in traditional standard-setting bodies and open-source represent a challenge.[136] Moreover, the different institutions might not all comply with the WTO rules, e.g. related to openness, consensus and transparency, which apply to standard-setting bodies (see also above).

Finally, there is still the threat that closed Open RAN proprietary and eventually incompatible, but better-performing solutions might emerge driven by closed consortia of a few strong players, which eventually does not allow the scaling up or broad deployment of their solutions, but might also limit the implementation of the O-RAN Alliance solutions. In addition, Huawei is yet not involved in the O-RAN Alliance, which creates some level of uncertainty.

Scenario IV: 5G for Big Tech

In this scenario, Big Tech companies become dominant in general, but consequently also in standardisation. On the one hand, their influence in the O-RAN Alliance might become bigger reducing the relevance of existing players. However, these players could on the other hand start offering alternatively non-O-RAN proprietary solutions.

---

135 Pohlmann et al. (2020), but also different Open-source licenses (Blind & Böhm 2019)
136 Blind & Böhm (2019)

As the last mile is expected to remain under the control of the MNOs, there is an opportunity for (far) edge cloud services. Especially, as O-RAN is based on cloud technology, reuse of O-Clouds, to more general Edge Cloud Service can be envisaged. O-Clouds are understood as infrastructure element (or collection elements) that is based on COTS servers, uses hardware accelerator add-ons as needed, and has a software stack that is decoupled from the hardware.[137] Consequently, the MNOs and the Big Tech companies have complementary interests, e.g. in cooperating in campus and industry networks, which might lead to common standardisation efforts in particular within the O-RAN Alliance.

However, due to the technological and financial strength of the Big Tech companies, there is a threat that the influence on MNOs within standardisation under the roof of the O-RAN Alliance might be reduced. They are already very active in Open-source software development.[138] Therefore, they might be able to leverage this asset also into the development of specifications within the O-RAN Alliance. Finally, their financial strength allows them to overtake existing players and to create powerful new entrants to eventually increase their influence in standardisation. It is important to note that this development cannot be prevented by slowing down Open RAN deployment in Europe. On the contrary, inactivity could result in a higher risk of technological disruption from the outside, as other markets are already moving dynamically towards Open RAN.

Overall, Big Tech companies may turn to be new competitors to MNOs across the entire value chain from RAN over the Core Network to Apps/Services. This competition might be distorted due to asymmetric regulation, in particular restricting the European MNOs. In addition to increasing their influence in the development of open standards and specifications, there is the risk that the Big Tech companies eventually close the originally open standards and turn them in follow-up generations into closed proprietary solutions excluding the MNOs.

The vendors perceive no additional opportunities in the context of standardisation within this scenario. However, standardisation is perceived as an important element to provide stability, because the returns to investment in standardisation will be generated only after five or ten years. Therefore, short term opportunistic behaviour and strategies of single players including the Big Tech companies are unlikely.

If standardisation remains the same, i.e. having the focus in 3GPP, then the vendors perceive little threats. If 3GPP will become irrelevant, then there will be no global standards and fragmentation will increase. However, this scenario might be dangerous for the vendors, because they fear that Big Tech companies are interested in controlling Open RAN. Therefore, the need for interoperability might be much lower. In addition, the Big Tech companies might not only operate networks but also supply their components, which create strong competitive pressure for the traditional vendors. If the Big Tech companies leverage their involvement in standardisation into the product market competition via specifying the open standards in their interest or even via developing proprietary interfaces, then the other incumbent vendors are threatened, and start-ups face very high entry barriers.

In addition to the increasing competition from the Big Tech companies, further competitive threats might come from Chinese companies, which are already heavily active in the O-RAN Alliance.

The scenario has some opportunities and threats from the 5G ecosystem perspective. The O-RAN ecosystem can potentially benefit from the Big Tech companies engaging in standardisation within the O-RAN Alliance, as they would provide additional momentum to the rise of O-RAN. Unfortunately, all these players are from outside Europe, thus the relevance of Europe will decrease. It is thus all the more important to quickly pool resources in Europe, including major vendors, MNOs and specialized industry, to build up a European critical mass in standardisation. Europe still maintains

137 O-RAN Use Cases and Deployment Scenarios WhitePaper, February 2020 (https://www.o-ran.org/resources)
138 Blind et al. (2021)

an advantage over the US in RAN equipment. However, the increasing transition towards cloudification means, that EU vendors need to adapt their current business model at a much higher speed than previously expected.

The entry of the Big Tech companies generates more competition and eventually lower prices, which is beneficial in the short run for the MNOs in the EU. However, this increased competitive pressure can be harmful to EU RAN equipment suppliers and may challenge the EU supply ecosystem in the long run. In particular, the potential double role of Big Tech companies as operators and equipment vendors is challenging EU vendors and EU MNOs. Common open standards and specifications developed under the roof of the O-RAN Alliance allow competition between MNOs in the EU and Big Tech companies also in offering services, which might be beneficial for the customers. The EU ecosystem will suffer if the EU MNOs will significantly lose market shares, because then in the long run their influence in standardisation will be reduced. Over time, multiple non-interoperable silo-solutions might emerge and the Big Tech companies have the option to increase customer loyalty via reduced interoperability as already successfully realized e.g. in charger interfaces. Eventually, due to geopolitical considerations, governments might make use even of originally open standards and specifications developed both under the O-RAN Alliance and 3GPP.

j. Economic impact for Europe

Information and communication technologies such as 5G generate two types of economic impacts (OECD 2003):

- First, the direct impacts in terms of value added and employment generated by equipment manufacturers, software and consultancy firms, and telecom operators.
- Second, indirect impacts (knock-on effects) generated in the use sectors where ICT help these firms to provide new services, become more productive and grow their value added and employment.

While the first effect is confined to mobile network operators and equipment manufacturers, the second effect can encompass all sectors of the economy where mobile services are used. However, the indirect effect is also more difficult to measure. The main channel of the indirect effect is productivity growth — firms achieve more output per unit of inputs. Productivity increases when firms make good use of ICT and can generate more value added with the help of digital technologies. A key challenge, however, is that productivity is often difficult to observe directly because there are many possible influences on productivity, and it is often difficult to separate and isolate the effects of these factors.

The evaluation of productivity effects from ICT also becomes difficult because of the complex relationship between ICT, productivity and economic outcomes (Van Roy et al. 2018; Harrison et al. 2014; Autor and Salomons 2018): New technologies are labour-friendly in principle, but higher productivity may also lead to automation and a loss of employment. Some well-received contributions on the economic effects of artificial intelligence (Frey and Osborne 2017; Arntz et al. 2016) and robots (Acemoglu and Restrepo 2020) stress this negative employment effect.

Direct impacts

The direct impacts of 5G manifest themselves in the turnover and employment of equipment manufacturers and telecom operators. The figures below show both indicators for total telecommunications services (NACE 61) and wireless telecommunications activities (NACE 61.2). We see that both indicators remained quite flat in the last 10 years; both sectors today employ less staff in 2018 compared to 2008. So, there is no evidence that previous introductions of new mobile network technologies have given a boost to turnover or employment.

The flat curves also indicate that productivity in terms of turnover per employee remained stagnant in the sector. However, we have to consider here that prices for mobile services decreased considerably during this period; therefore, there may be productivity gains in physical terms (e.g. traffic volume per employee) but these increases could not be turned into productivity gains in monetary terms.

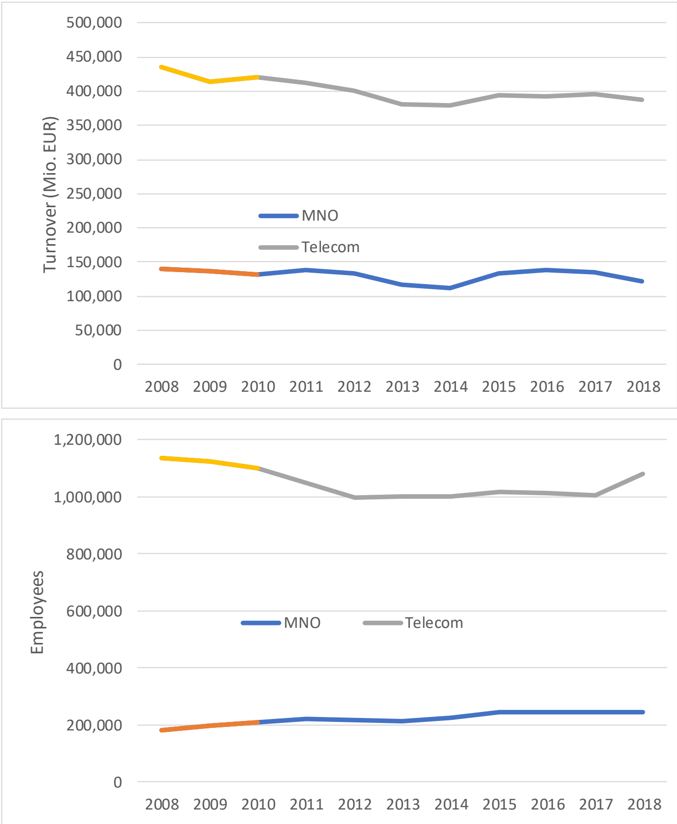


Figure 6: Turnover and number of employees in MNOs and the wider telecommunications sector, 2008-2018.[139]

A similar picture emerges for the producers of communication equipment (NACE 26.3) in Europe. The number of persons employed in this sector decreased from around 264,500 in 2008 to 138,037 in 2018 according to Eurostat Structural Business Statistics. A similar development, from 100 bn. EUR to 49 bn. EUR can be observed for turnover between 2008 and 2018. So, the industry almost halved during one decade. It is difficult to see a positive economic effect of 4G in these numbers. This development can be attributed to employment and turnover losses in the German, Italian, Hungarian, Finnish and Swedish communication equipment industry, which is related to the decline of the European mobile phone industry.

The data do not allow to distinguish between the producers of mobile phones and telecom equipment. In the case of Nokia, Ericsson and Siemens, they were the same firms during this period. We can see a positive trend only in very few countries, most notably Poland. Thus, a positive economic effect of 5G on the European manufacturers of telecom equipment and European MNOs would be a reversal of the trends we have seen in the last 10 years.

139 Note: Data for 2008-2010 refer to the European Union without Croatia; Source: Eurostat, Structural Business Statistics

Indirect impacts

Possible indirect effects of 5G originate from the contributions of 5G to product, process, and service innovation in European firms, which in turn increase labour productivity. Like in the case of direct effects, the effects of previous generations of mobile communication are not visible in productivity trends. Labour productivity growth has been flat in the EU, with a growth rate of less than two percent annually since the Financial Crisis of 2008/09. The introduction of previous generations of mobile communication did not seem to impact the growth rate in the past.

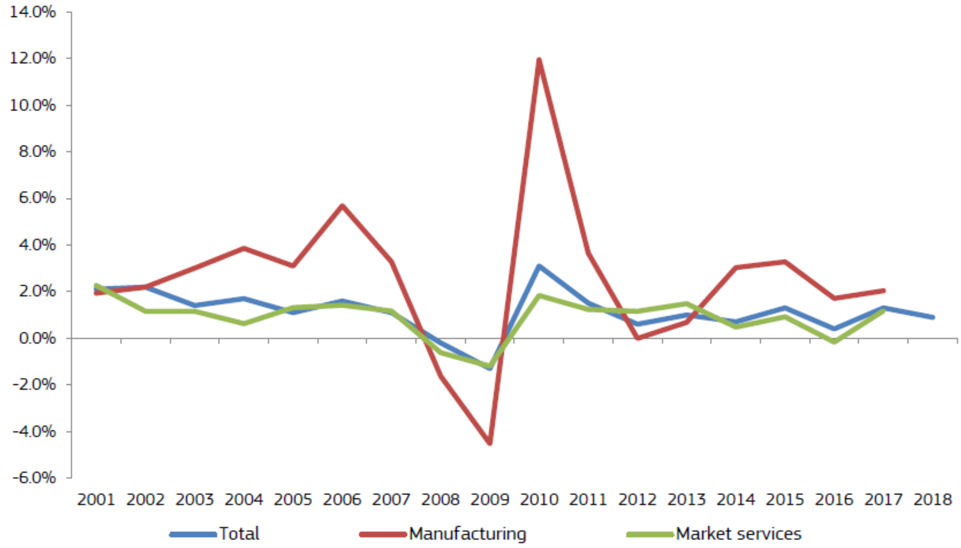


Figure 7: Annual change of labour productivity in the European Union, 2001-2018[140]

There are nevertheless some studies which claim a big economic effect of 5G for the future. Boston Consulting Group (BCG 2021) expects that 5G will contribute between 1.4 trillion to 1.7 trillion USD to US gross domestic product (GDP) and 3.8 million to 4.6 million new jobs until 2030. These gains amount to around one percent of total GDP of the US in 2024 and increase to around two percent in 2030. US GDP for 2021 is expected to be around 21.9 trillion USD. The largest gains are expected in information services, manufacturing, professional services, and construction.

Another recent study comes from the consultancy PricewaterhouseCoopers (PwC 2021). It includes five sectors - healthcare, smart utilities, consumer and media, industrial manufacturing, and financial services - and finds that the adoption of 5G will add 1.3 trillion USD to global GDP by 2030. Readers will note that this is the amount estimated by BCG for the US alone.

An older study for the European Commission (Tech4i2 et al. 2016) estimates total economic benefits of 5G to be 113.1 billion EUR per year in 2025. An estimate of the GDP of the European Union for 2025 is around 17,000 billion EUR, so this amounts to around 0.6% of the GDP of the EU. The lion’s share of these benefits will occur in four industries: automotive, healthcare, transport, and utilities, which together account for benefits of 62.5 billion EUR in 2025. Second-order benefits in several other sectors sum up to 50.59 billion EUR. 63 percent of these benefits will arise for business, and 37 percent will be provided for consumers and society. Annual benefits in 2030 are broadly the same as in 2025.

A study for Australia (2018) estimates that 5G could add 1,300 to 2,000 AUSD in GDP per capita after the first decade of the rollout. Australia’s GDP per capita will be around 95,210 AUSD in 2025,

140 Source: EU KLEMS 2019

according to an estimate by the International Monetary Fund, so 5G will increase Australia's GDP by roughly one to two percent in 2025.

To sum up, previous experience with the economic effects of 4G indicates that we should not expect too much from 5G. Nevertheless, studies that investigate possible effects are optimistic and expect that 5G will add one to two percent to gross domestic product each year from 2025 to 2030.

Scenario-specific assessment

The four different scenarios also lead to different impacts of 5G on Europe's economy. In general, economic benefits for Europe should be higher in scenarios with a faster roll-out of 5G, and lower in scenarios with a slower roll-out. Similar differences have been reported for Australia (Commonwealth of Australia, 2018).

In scenario I, **Incumbent players driving 5G**, we expect a continuation of the trends we have seen in previous years for Europe's telecom provider and equipment manufacturers, which was mainly flat. This means that the contribution of 5G will be the same as the current contribution of 4G technology to Europe's economic growth. However, new providers of services based on 5G may emerge which can foster growth.

Scenario II, **Slow pace of 5G Roll-out**, assumes the slowest roll-out for 5G of all scenarios, with adverse effects for overall economic benefits of 5G. However, the slow roll-out in this scenario may partly be compensated by the favourable conditions for European suppliers of 5G equipment. Nevertheless, we believe that negative effects from a delayed roll-out are larger than the positive effects for European suppliers in this scenario.

Scenario III: **Open RAN as a game-changer**, and Scenario IV: **5G for Big Tech** offer some potential for the European economy thanks to the emergence of a vivid services eco-system which will be the key driver of economic growth. Studies on the economic impacts of 5G have shown that these are largest when 5G diffuses fast. If Industry 4.0 is a fast-growing use case, it may provide opportunities for Europe's large manufacturing base in particular. Several industrial firms may extend their product range to 5G based services. But there are also risks for Europe associated with these two scenarios. For example, the fast diffusion of Open RAN may allow non-EU companies to take a good part of the MNOs and suppliers market. This seems most relevant in Scenario IV. Growth in these two scenarios will also be spurred by new market entrants for services and an overall growth of the 5G ecosystem. However, given the weak market position of Europe in many software and services markets, it seems uncertain if companies rooted in Europe can make the best out of these new opportunities. Much will depend on the question if non-European firms will adopt these new businesses via European affiliates directly from their home countries.

4. Overview of Existing Policies

Policy options to foster a secure and economically viable 5G supply-ecosystem for Europe can include a re-enforcement or re-configuration of existing measures and the inclusion of new policy measures.

In this section, we first provide an overview of existing policy measures for advancing the 5G ecosystem. The overview is based on a review of relevant academic literature as well as policy documents and information provided by the 5G Observatory, including the 5G conference in February 2021.[141] We identified the most relevant and recent policy measures related to 5G. We then attributed the policies according to the innovation policy instrument framework as far as this was possible. [142]

Based on this review of the literature related to innovation policy in a wider sense[143], but also to policies related to foster innovation ecosystems[144], the results of screening existing policies related to 5G, scientific papers and the interviews with the stakeholders, we then derived preliminary policy recommendations.

a. Direct support for business research, development and innovation

According to the 5G Observatory website, the EU has supported the development and deployment of 5G through several funding instruments, including the Connecting Europe Facility - Telecoms, the Digital Europe programme - Strategic and R&D Investment and the 5G Public Private Partnership (5G PPP). More recently, 20% of the EU's € 672.5 billion COVID-19 stimulus package, delivered through the Recovery and Resilience Facility, has been earmarked for digital transformation, including the roll-out of fast broadband services.[145]

In addition, support has been provided for the development of 6G, with Nokia being tasked with leading the EU's Hera-X project, which is the flagship of the European Commission's 6G research initiative.

b. Entrepreneurship policy

There are certain frameworks to help entrepreneurs in the EU, e.g. EntreComp: The Entrepreneurship Competency Framework. There is also the European Electronic Communications Code (EECC), which supports the entry of new players for 5G by facilitating spectrum sharing, trading and leasing. However, there may be a lack of specific measures for 5G entrepreneurship in the EU, as a brief overview of 5G start-ups on Crunch Base shows that they are predominantly US-based.

c. Technical services and advice

EU agencies and institutions have developed together with the Member States guiding documents with technical advice, such as the "Toolbox of risk mitigating measures (2020)" of the NIS Cooperation Group, which addresses 5G cybersecurity issues both from the strategic and technical angle. The European Union Agency for Cyber Security (ENISA) has also issued technical guidance on the implementation of the "Toolbox" and on the security requirements of the European Electronic Communications Code (EECC) to support Member States in strengthening 5G cybersecurity.[146]

141 https://5gconference.eu/
142 Edler and Fagerberg (2017)
143 Edler and Fagerberg (2017)
144 Grandstrandand Holgersson (2020); Rinkinen and Harmaakorpi (2019)
145 Gilles and Toth (2021)
146 Milenkovic and Dekker (2020)

d. Cluster and innovation network policy

The 5G PPP could be considered a cluster, defined as locally embedded groups of firms and other organisations such as industrial districts or spaces and regional innovation systems.[147] The creation of the 5G PPP between the European Commission and the European ICT industry with its trials and development of use cases can also be classified as an innovation network. In the 5G PPP, public funding is matched by significantly more private funding in the creation of 5G trials as well as the creation of 5G cross-border corridors in building a 5G ecosystem in Europe as well as a supply chain for 5G hardware (EC website 2020). Specific clusters include, for instance, Germany's automotive industry cluster, Estonia's marine industry cluster and Finland’s Industry 4.0 cluster.[148]

e. Policies to support collaboration

EU cluster policies are best reflected in the 5G PPP and spectrum sharing, leasing and trading facilitated by the EECC.[149] However, to reduce the risk of 5G rollout, it would be advisable to try to ensure that MNOs coordinate and pool their resources in building 5G infrastructure, as well as using the joint deployment with other infrastructure projects where possible.

f. Policies to support private demand

5G has been marketed as central to future car and mobility (e.g. driverless cars), entertainment (e.g. high-speed media content), smart cities, smart agriculture (e.g. precision farming), industry 4.0 (e.g. industrial IoT) and health (e.g. remote surgery).[150] However, demand for 5G is less clear-cut, as it depends not only on the realised level of the 5G rollout but also, and more importantly, that alternative technologies that are sometimes even more suitable. So far, we cannot observe a clear-cut case of consumer demand for 5G-related products.[151] For example, in the case of Industrial IoT, there are alternative technologies well suited for applications; applications that meet industry demand a very long-range, low cost, low data capacity, service (i.e., situations for which 5G is not needed). Furthermore, unlicensed spectrum may often be more attractive for IoT applications, particularly where industry users might prefer controlling their private networks as opposed to renting from a public 5G network.

Still, the case for 5G is made more visible through the various 5G trials taking place in the EU, including cross-border corridors. Another example would be smart agriculture with precision farming, which would help eliminate waste to work more sustainably. However, 5G is not essential here either, because LoRaWAN could be used instead.[152] Nevertheless, there are advantages to having everything work over one network/technology like 5G, even if there are alternative technologies. One of the more valid cases would be for IoT devices for a smart home. However, there is a risk that due to a possible lack of interest, and especially in light of recent privacy and security scandals, consumer trust and thus the adoption of IoT devices may decrease.

The lack of private demand for 5G technology or networks has been addressed by a few policy initiatives at the level of the Member States. For example, the Federal Ministry for Economic Affairs and Energy in Germany supports more than one hundred partners in the various projects with a total of EUR 50 million to support campus networks in companies and research institutions. In May 2021, Germany and France together launched a new call for common projects for 5G applications and private networks.[153]

147 See Uyarra and Ramlogan (2016).
148 Gilles and Toth (2021)
149 Pujol et al. (2021)
150 Gilles and Toth (2021)
151 Blackman and Forge (2016)
152 Bieser et al. (2020)
153 https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2021/05/20210525-Deutschland-und-Frankreich-starten-Foerderaufruf-zu-5G-Anwendungen-und-privaten-Kommunikationsnetzen.html

g. Public procurement policy

Public procurement policy regarding 5G is strongly influenced by cybersecurity concerns.[154] This is because 5G will not only play a more crucial role in our lives than previous network technologies, e.g. the use of 5G for utilities and critical infrastructure, but also the exponentially greater collection and processing of personal data.[155] The European Commission, therefore, issued a recommendation on the "Cybersecurity of 5G" in 2019, calling on the Member States to conduct and submit national risk assessments. Subsequently, the EU 5G Cybersecurity Toolbox was outlined, to guide the Member States in addressing key 5G-related cybersecurity risks.[156] The Toolbox has a specific Supporting Action (SA10), which addresses public procurement at the EU and the national level. SA10 outlines guidelines for 5G-related security provisions in public procurement and EU funding programmes. Key proposals in the SA include assessing the risk profile of suppliers and putting in place restrictions on suppliers considered to be high-risk and ensuring a diverse supply chain. In addition, the EU Cybersecurity Act strengthens ENISA’s power and calls for the development of certification schemes for digital processes and products, including those relevant to 5G networks.

Procurement policies in the EU Member States have responded to this to varying degrees (national security is the prerogative of individual EU Member States).[157] For example, Sweden has banned the use of 5G equipment from Huawei and ZTE for its 5G network. Orange and Proximus have chosen Nokia for rolling out their 5G networks in Belgium and Luxembourg following US pressure.[158] Other EU Member States have not completely banned Huawei or ZTE as equipment suppliers, but have subsequently still been careful to limit their dependence and procurement of their equipment. This helps their competitors, especially Nokia and Ericsson, but recently the four major MNOs in Europe signed a Memorandum of Understanding to prioritise “Open RAN”, benefiting other companies, including smaller ones, as well as US tech companies, and limiting the dominance of Ericsson and Nokia.[159] In terms of policies, this could be positive for the EU to maintain a diverse ecosystem of players and in line with the recommendations of its security toolbox, but at the cost of undermining the solid position of EU vendors and the EU technological autonomy. It would also mitigate the risks of high dependency on specific vendors and allow greater pathways for innovation.[160] On the other hand, there are other geopolitical and competition concerns. Open RAN could favour companies from other countries at the expense of European ones, which is particularly problematic as it might benefit large US tech companies that already dominate much of the global digital markets. Moreover, there is a clear national interest in this, where, for example, in the US, whose companies are not major players in the deployment of 5G equipment, a law was recently passed authorising $750 million in public funding for the development of Open RAN technologies.[161] Furthermore, the logic of a diverse ecosystem of players and suppliers is also to ensure cybersecurity goals. EU device suppliers that can be directly regulated and monitored under EU law would address a wide range of cybersecurity concerns, especially concerning espionage and sabotage by foreign states.

h. Standardisation

Standards are central to the 5G ecosystem and play a key role in the interoperability of global telecommunications networks.[162] The most important standardisation body in the development of 5G standards is the 3rd Generation Partnership Project (3GPP), which comprises a variety of different standard development organisations. Standardisation is still ongoing, but the first two phases of 5G standards have already been completed and published. The first phase was 3GPP Release-15, the

154 Stuchtey et al. (2020)
155 Cf. Kleinhans (2019)
156 NIS (2020)
157 Blackman and Forge (2019)
158 Reuters (2020)
159 Cerelus (2021)
160 Kagerman et al. (2021)
161 Cerelus (2021)
162 EU ICT rolling plan (2021)

second 3GPP Release-16. The latter release, for example, was critical in delivering the standards needed for a wide range of use cases. The complexity and ubiquitous and interoperable nature of 5G means that the 5G standardisation ecosystem requires extensive stakeholder and international collaboration, with strong consideration of the inherent competing interests of stakeholders (e.g. who owns the standard-essential patents (SEPs)) and cybersecurity concerns. As a global view of 5G has been outlined at the international level by the International Telecommunication Union (ITU) and several joint declarations have been signed between the European Commission and other nations (e.g. China, Brazil, South Korea and Japan), the EU has adopted a policy of international cooperation on 5G. The 5G PPP between the European Commission and the European ICT industry represents another case of cooperation, one which helped to test 5G technology and use cases, and contribute to the development of 5G standards (Rolling Plan, 2021).

The EU 5G Security Toolbox is an important measure to secure 5G networks and also relates to 5G standards. In response to a technical measure (TM02) of the Toolbox calling, "...on competent authorities in the EU Member States to ensure and assess the implementation of security measures in existing 5G standards (specifically 3GPP) by operators and their suppliers", ENISA subsequently published the "security in 5G specification report- Control in 3GPP".[163] This report shows the Member States how to implement the technical measures and serves to further inform relevant authorities about the standardisation environment concerning 5G.

i. Regulation

For 5G, one of the main regulatory concerns has been spectrum regulation. As the rollout of 5G is associated with high-risk initial investments, increased complexity and the importance of maximum coverage, more effective use of spectrum has proven essential. Sharing spectrum (e.g. the RAN) or effectively leasing or sub-leasing operator spectrum are possible solutions. These could help to reduce the risk of 5G deployment, which helps develop use cases and drives innovation, and maximise coverage, which in turn could facilitate uptake. At the EU level, the European Electronic Communications Code (EECC) came into force in 2018 - Member States have two years to transpose it into national law - which addresses spectrum usage issues. For example, the EECC facilitates spectrum sharing, trading, and licensing and promotes risk-sharing for major network rollouts (Pujol et al. 2021, p. 15). Another important regulation in the context of 5G is the EU's Cybersecurity Act, which gives ENISA more powers and resources. It also enables an EU-wide ICT certification scheme framework (e.g. for products) about cybersecurity concerns. National policies vary, but in Finland, for example, there is the 5G Test networks Finland (5GTNF), which is a collaboration among academia, industry and government, providing an environment for testing and researching 5G and bringing regulatory and technical coordination (IDB, p.30).

j. Technology foresight

The European Commission has invested in foresight exercises related to 5G to better understand its opportunities, but also its threats on the one hand and possible drivers and barriers considering also the different kinds of uncertainties on the other hand. The need for foresight activities is even further justified because 5G marks a significant change from previous mobile network technologies, being seen as more than simply a next-generation technology and instead acknowledged as a completely new way of approaching communication systems (OECD 2019, p.6). However, the success of 5G and the resulting potential benefits will depend on its adoption, the level of acceptance and sufficient adaptation of regulatory structures, as well as the development of new business models (ibid., p. 5). Use cases are central to driving 5G and have fostered greater collaboration than for previous network technologies (e.g. the EU 5G corridors). Future regulatory concerns will need to address issues of network densification and slicing, as well as power density. Therefore, comprehensive foresight activities have been conducted related to 5G, including the current study, to guide the other policies.

163 Milenkovic and Dekker (2021)

5. Policy recommendations

Establishing a viable 5G supply ecosystem requires a carefully considered combination of system-oriented policy measures, which should ultimately contribute to the following overarching goals derived from objectives of different EU policy domains:

- The EC and the EU Member States should develop an open and secure 5G ecosystem in the long run, which includes MNOs, incumbent and new European vendors, software providers, Open-source communities and European users from vertical industries.164
- The EC and the EU Member States should promote European digital autonomy and technological sovereignty via closer collaboration between the participants of the 5G ecosystem and a strong approach towards open specifications.165

The policy recommendations we specify below seek to reflect the complexity and diversity 5G supply market issues by consolidating: a wide range of viewpoints based on the baseline analysis[166]; statements by experts interviewed in the context of the assessment of the four scenarios (see chapter 3); the review of the existing policy measures (see chapter 4); and the results from the second stakeholder workshop on 19 May 2021.

In the stakeholder workshop, a set of preliminary policy options were presented and assessed by participants and the expert panel. In the morning session of the workshop, more than 200 specific suggestions to a set of predefined policy areas, which are going to structure our policy recommendations were made. In the afternoon session, 44 experts were separated into four groups, one for each of four scenarios, to discuss scenario-specific policy measures. While the resulting suggestions are integrated with the policy recommendations, along with the scenario-specific measures and associated prioritizations and assessments, the policy measures below mainly rely on the frequency mention, as morning session responses did not go into detail.

Guided by taxonomies of innovation policy instruments and prior work[167], we structure the specific policy recommendations related to the 5G ecosystem along the following domains: 1) Human Capital Development, 2) R&D, 3) Standardisation / Testbeds / Certification, 4) Entry of New Players, 5) Public Procurement and 6) Regulation.

a. Human Capital Development

The relevance of human capital for a functioning innovation system is fundamental, in particular in the area of 5G technologies, where the involvement of skilled personnel is key not only in research but also in standardization.[168] Although we have not explicitly focused on the educational aspects in our assessment of the scenarios, we have evidence from the Community Innovation Survey[169], that the lack of skilled labour is an important barrier for innovation for European companies in the ICT sector. As mentioned above, the participants of the morning workshop were invited to provide suggestions on policy recommendations to support the future of 5G supply market via a live online survey. There, it was noted that it is essential to attract young people, from an early age, to pursue education in the fields of Science, Technology, Engineering, and Mathematics (STEM). For the advancement of skills, a general promotion of education in STEM fields and the development of digital (programming) skills from primary school to higher education was suggested. Regarding higher education, participants mentioned a specific need for increasing skills in virtualization technologies and network innovation, as well as for the provision of schemes between universities

164 See for example Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G from 2019 or Commission Recommendation of 26 March 2019 on Cybersecurity of 5G network.
165 Strengthening the digital sovereignty of the EU was one of the four priorities for the German Presidency of the Council of the EU in 2020 (Federal Ministry for Economic Affairs and Energy 2020)
166 See Taga et al. (2021)
167 See Blind et al. (2021) in recommendations to support Open-source in the EU
168 See for example Pohlmann et al. (2020)
169 Biagi et al. (2016)

and SMEs to develop cloud-native telecom skills. Based on these insights, we derive the following recommendations:

- Consider open and interoperable 5G network development and design topics into the European Qualifications Framework (EQF) as well as Master programmes covering 5G technology including addressing the security dimension. This recommendation reflects the need to remedy the increasing shortage of skilled experts in the EU, particularly in comparison to Asia and the US. (Target audience: EC).
- Promote inclusion of open technology approaches, including Open-source (development, business models and licensing), in Master programmes that address 5G technology (Target audience: Member States and their organisations responsible for such education).
- Incentivize Higher Education Institutes (HEIs) and Public Research Organisations (PROs) in general and business schools in particular to offer specific management courses related to 5G technology, e.g. as mini MBAs to address the need for vocational education (Target audience: Member States).
- Launch an EU-wide accepted and vendor-independent certification scheme for experts with skills in 5G technologies, incl. cybersecurity, to increase the functioning of this labour market (Target audience: EC).

b. R&D

Public support of R&D investments is needed in the EU across the whole supply chain of 5G, from basic research over experimental development, trials and pilots to large-scale deployment, to correct market failures in such domains generated by the public good characteristics of such infrastructures and the positive externalities generated by R&D in general. In addition, the investments in the EU in 5G technologies and networks are lagging beyond those in particular Asian countries, which is challenging the EU's competitiveness.

Due to the positive externalities generated in research collaborations and the objective to reduce the dependency from very few vendors in the 5G supply chain, R&D funding should allow for structured and stable collaboration with leading universities and research institutes to strengthen the innovation system including the internalization of knowledge spillovers. Furthermore, several comments noted difficulties for SMEs to participate in publicly funded R&D actions, and the resulting need for grant schemes supporting individual research efforts, but also specific target groups such as smart cities and regions. Other suggestions focused on the exploitation of synergies and the promotion of 5G solutions, including the need to support specific topics such as cloud-native technologies, Artificial Intelligence, Machine Learning, privacy, and 5G/6G security.

Based on these suggestions, we derive the following recommendations:

- Provide more R&D funding focusing on 5G and Open RAN through existing programmes, such as Horizon Europe at the EU level, but also research programmes launched by the Member States. New R&D funding initiatives focusing on 5G should in particular target SMEs, but also start-ups, microenterprises and individuals (Target audience: EC and Member States).
- Launch in particular an open call within the context of "Important Projects of Common European Interest"[170] related to 5G including Open RAN, following the IPCEI on Microelectronics (Target audience: EC).[171]
- Support R&D projects related to 5G, with a focus on the collaboration between large and small companies, including start-ups, located in the EU to promote the 5G ecosystem in the EU (Target audience: EC and Member States).

170 IPCEI https://ec.europa.eu/commission/presscorner/detail/en/IP_21_689
171 https://www.ipcei-me.eu/

- Support the development of regional clusters of excellence or smart cities in the area of 5G technologies, networks and applications, e.g. in the context of the European cluster excellence programme. Such clusters could consist of partnerships between industry, academia, research institutions, Open-source communities and the private sector and might include the co-funding of the needed 5G infrastructure, e.g. via Public-Private-Partnerships (Target Audience: EC, Member States and regional authorities).
- Support the identification and development of business models or use cases for verticals related to 5G networks and applications via competitions (Target audience: EC and Member States).

c. Standardisation / Testbeds / Certification

Standardisation and the resulting standards, testbeds and certifications are crucial for the development of mobile telecommunication networks, as is shown by the massive efforts in 3GPP and the different releases of 5G standards as well as the creation of the O-RAN Alliance in 2018. To avoid fragmentation or lacking interoperability in 5G networks, the required standards should not be developed at a national or European level, but only at a global level. With ETSI, the EU established more than 30 years ago a globally accepted institution, which can help the EU also within 3GPP to remain in a leading position in 5G-related standardization activities. For the development of a functioning 5G ecosystem, open and transparent standardisation processes and interoperable standards are necessary. Standardisation activities and the related standards have to be complemented by attractive testbeds[172] and accepted certification schemes. Consequently, the following recommendations are derived:

- Investigate the compliance of the O-RAN Alliance to the Code of Good Practice when developing standards released by the WTO and the EU Regulation No 1025/2012. The O-RAN Alliance could make proposals to assure its compliance as part of this process (Target audience: EC).
- Consider a closer collaboration between 3GPP and ETSI on the one side and the O-RAN Alliance on the other side that starts with an MoU but eventually aims at accepting O-RAN Alliance specifications as ETSI standards via a fast track procedure (Target audience: EC, 3GPP/ETSI and O-RAN Alliance).
- Provide support for all stakeholders, but SMEs and start-ups in particular through open test-beds in all Member States. This includes interoperability testing, i.e. bringing together operators and suppliers to test equipment in networks (e.g. following the experience of ETSI plugfests, but also the 5G Supply Chain UK Diversification Strategy), deployment, and certification labs related to the specifications of the O-RAN Alliance. The goal is to identify standards gaps, to develop new standards, to enhance existing standards or to develop, test, and demonstrate standards in an Open-source process173 (Target audience: EC and Member States).
- Support the creation of open platforms for experimentation, e.g. to support 5G experimentation by factories in the context of Industry 4.0 or 5G campus networks (Target audience: EC and Member States).
- Consider the development of a platform (e.g. a systems integrator platform) that solely relies on European players and that provides different supplier options especially for smaller operators. In this context, the already existing 5G Infrastructure Public Private Partnership (5G PPP) should be considered as starting point for the development of such a platform (Target audience: EC).

172 For example, the UK has launched a programme supporting testbed related to 5G https://www.gov.uk/government/publications/5g-testbeds-trials-programme-update, but also Finland https://5gtnf.fi.
173 Koch and Blind (2021): Towards agile standardisation: Testbeds in support of standardisation for the IIoT, IEEE Transactions on Engineering Management 68 (1), 59-74.

- Establish a European Certification Scheme applicable for components and products related to 5G. Such a scheme should include also O-RAN Alliance specifications and address security issues in coordination with the requirements by ENISA (Target audience: EC).

d. Entry of new players

The diversity of an ecosystem benefits from the entry of start-ups, but also of already established companies from other domains, which have been active in the telecommunication sector in the past. They might have still relevant expertise in particular in producing telecommunications equipment. In addition, technological sovereignty[174] or digital autonomy of the EU can be strengthened by European companies that enter the 5G ecosystem by reducing the dependency on large tech companies from outside Europe. However, start-up activities in the EU are lagging behind those in the US and Asia. Therefore, we derive the following recommendations:

- Launch 5G/Open RAN specific programmes to foster entrepreneurship in 5G related technologies and business models. They can be linked to the Startup Europe Partnership (SEP), which is building bridges between Europe's start-up, corporate, education institutions and investment communities and is already supported by several EU-based MNOs (Target audience: EC and Member States).
- Continue the Enhanced EIC programme (including the EIC Accelerator) and open it to applications from young, high-risk, R&D-intensive entrepreneurs that focus on 5G-related technologies and business models to address the lack of venture capital in the European small business ecosystem caused by the higher risk aversion of private European venture capitalists (Target audience: EC).
- Provide venture capital to 5G-related start-ups (including spinoffs from public research organisations) in the context of the European Innovation Council Fund175 or the Connecting Europe Broadband Fund176, which has recently invested in a Dutch start-up developing satellites for IoT applications (Target audience: EC).
- Develop new schemes that support start-ups and small companies in developing products relevant for 5G (including the Open RAN architecture).

e. Public Procurement

Public procurement, in general, is seen to be an appropriate tool for stimulating innovation and growth from the demand of the public sector. In particular, the public procurement of networks and their components was deemed to become increasingly important to strengthen the European supplier landscape. In addition, private networks are becoming relevant, e.g. for railroads or public protection and disaster relief, often bypassing mobile network operators. In this context, the Member States are particularly relevant to consider 5G technologies and their applications in their public procurement strategies. To avoid fragmentation and lack of interoperability, standards play an important role in public procurement, i.e. the specifications should reference international or European standards. Based on these considerations, we derive the following recommendations:

- Encourage public procurers to open their tenders to radically innovative 5G solutions, which may have a high risk of failure, focusing on EU suppliers (Target audience: EC and Member States).
- Exploit the potential synergies between commercial procurement and standards related to 5G technologies by referencing 3GPP and O-RAN Alliance specifications and standards instead of company-specific proprietary specifications related to 5G technologies. The procurement processes should follow EU-wide public procurement guidelines and recommendations, particularly taking into account the needs of SMEs and start-ups (Target audience: Member States, regional authorities and companies).

174 Edler et al. (2020)
175 https://eic.ec.europa.eu/index_en
176 CEBF https://www.cebfund.eu/

- Exploit the potential synergies between commercial procurement and 5G-related Open-source technologies more strategically and systemically, i.e. not only reference to open international standards, but also code available in Open-source repositories. In addition, these processes should take into account the specific needs of Open-source-based SMEs (Target audience: Member States, regional authorities and companies).

f. Regulation

Although standards are crucial for the success of telecommunication networks in general and 5G networks in particular, the regulatory framework plays an important complementary role. Regulations address different aspects, which eventually are also contributing not only to innovation in general[177] but also to an open and diversified 5G ecosystem and, eventually, to digital autonomy or technological sovereignty. The literature, the interviewed experts, and the participants of the stakeholder workshop suggested differentiating the regulations into three areas: 1) competition, 2) the protection of the demand side, i.e. security, and environmental protection, and 3) energy efficiency. Following two generic recommendations addressing technology neutrality and agile regulation conducted in international cooperations applicable to all types of regulations, recommendations are presented according to these areas:

- Specify all regulations - in particular in still emerging technologies, where not already European or global standards have been established - based on the principle of technology neutrality, which is also recommended by the OECD (2015) related to system innovations, to avoid biased and inefficient technological developments (Target audience: EC and Member States).
- Enable the development of agile regulation also in co-operation across Member States, similar to the focus on international instead of national standards, to address the regulatory challenges raised by dynamically emerging technologies, like 5G, and support socially beneficial innovations178 (Target audience: EC and Member States)

Competition

The regulation of competition aims at assuring a high level of competition in general, which not only fosters innovation but also allows the entry of new players. Competition regulation should prevent the abuse of dominance and monopolization of markets by specific companies, e.g. Big Tech companies or cartels. In addition to countries' internal perspectives, initiatives from foreign companies, such as acquisitions of companies and price dumping strategies, should also be considered. Furthermore, competition regulation should encompass liberalisation and competition intervention in regulated sectors and general pro-competitive policy reforms. In the context of 5G, an effective competition regulation can promote both the 5G ecosystem as well as digital autonomy and technological sovereignty.[179] We derive the following recommendations:

- Examine strategic take-overs of European companies, including start-ups, by large non-European companies in the context of Regulation (EU) 2019/452, a framework for the screening of foreign direct investments into the EU, and establish the option that the EC or the Member States hold a "golden share" of domestic companies (Target audience: EC).
- Check for dumping prices by non-EU vendors in the framework of the Regulation (EU) 2016/1036 on protection against dumped imports from non-EU countries related to 5G technologies and consider involving the WTO or set up countermeasures, e.g. establishing an EU fund for EU vendors (Target audience: EC).
- Foster competition between incumbent MNOs and new MNOs entering the market, e.g. by operating private or regional 5G networks. Competition regulation should cover spectrum

177 See e.g. Blind (2016) or McEntaggart et al. (2020)
178 See the recently public consultation on the draft OECD Recommendation on Agile Regulatory Governance to Harness Innovation https://www.oecd.org/gov/regulatory-policy/regulation-and-emerging-technologies.htm.
179 In general, universal access regulation is also very important, but not immediately for the improvement of the 5G diversity in the supply chain.

allocation, which needs to be more dynamic and coordinated at the European level to avoid fragmentation between Member States. Overall, the incentives to invest in 5G deployment should be increased, e.g. via fostering the entry of specialized systems integrators and verticals responding more effectively to heterogeneous customer needs (Target audience: EC in collaboration with the Member States and their regulatory authorities responsible also for spectrum allocation).
- Foster network sharing to push the rollout of 5G (Target audience: EC in coordination with Member States).

Security

Competition regulation addresses the supply side, which fosters higher levels of security due to competitive pressure. However, there are reasons to specifically protect the demand side, i.e. the users of 5G networks. Security characteristics of networks are generally not transparent to their users, i.e. information asymmetries exist, which already justifies the intervention of the regulator. In addition, security breaches or cybersecurity attacks generate negative network externalities for (indirectly) affected users, e.g. if passwords or other personal data have been compromised. Finally, incentives for investments in network security features are limited in open technologies, like Open-source, due to the free-rider phenomenon.[180] Overall, these three types of market failures are strong justifications for the implementation of security regulations, which also apply to 5G networks and their related services. Complemented by the suggestions of interviewed experts and workshop participants[181], we derive the following recommendations:

- Consider not only 3GPP but also the O-RAN Alliance, particularly their specifications and standards in the Cybersecurity of 5G networks EU Toolbox. This includes the strategic and technical measures, but also the supporting actions, in particular SA 10 on ensuring that 5G deployment projects supported with public funding take into account cybersecurity risks (Target audience: EC).182
- Support risk assessment schemes for vendors in the 5G supply chain based on clearly operationalized and transparent security regulations, which could be specified by complementary European or international standards (Target audience: EC in coordination with the Member States).
- Fund security audits of critical open technology projects, not only in the context of Open RAN but also of other 5G technologies that incorporate Open-source technologies and might require specific security-related improvements through public resources (Target audience: EC in coordination with the Member States).

Energy Efficiency

Improving energy efficiency is one option to reduce negative externalities for the global climate. Therefore, the 5G PPP initiative aims to reduce energy consumption by 90% by mobile communication networks where the dominating energy consumption comes from the RAN.[183] Environmental regulations are one instrument to address such negative externalities also in the context of 5G. Based on the suggestions of the interviewed experts and the participants of the stakeholder workshop, we derive the following recommendations:

- Consider the potential improvement of energy efficiency by including 5G technologies in future regulations and standards, e.g. via specifying energy-efficient targets for 5G

180 See Nagle et al. (2020)
181 In addition to regulations focusing on the protection of the consumers, the panel discussion also emphasized the empowerment of the demand side. However, this empowerment is only a "soft" approach, which might complement "hard" regulation.
182 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.
183 https://5g-ppp.eu/

complemented by financial incentives for energy-efficient solutions (Target audience: EC in coordination with Member States).

- Enhance R&I on the use of renewable energy sources for supplying network elements. Gathering environmental energy through dedicated harvesting hardware to supply 5G Base Stations can translate into operational expenditure savings and a reduction of the environmental footprint of mobile networks.184

In summary, the shaping and eventually the implementation of all these recommendations have to consider carefully the complexity and the tensions among the interests of the various stakeholders involved, but also of the public to realise the whole potential of 5G and eventually to increase the economic, societal and environmental welfare across Europe.

184 Lopez-Perez et al. (2021)

6. Conclusions

We close this report by putting current and ongoing policies and initiatives into conversation with the policy recommendations intended to support 5G and broader system innovations.

Heavy investments in 5G research, development, and innovation are observable in standard-essential 5G patent data of multinational vendors.[185] At this point and complementary to these standard-essential investments, public funding would do well to comprehensively support sector-specific applications of 5G technology (e.g., health or mobility). Business model innovation related to 5G technology should also be included in such public investment. However, the public funding has to shift its focus now to support innovation in the sector-specific applications of the opportunities of the 5G technology, e.g. health or mobility. Here, also business model innovation based on 5G technology should be included.

Although generic support for entrepreneurship is available at the EU level, additional and specific funds should be devoted to promoting start-ups seeking to a) contribute technologies or components to the 5G supply chain or b) develop sector-specific 5G applications. The need for 5G-targeted entrepreneurship is visible when comparing the limited number of startups relying upon 5G technology in the EU with those for Asia and the US.

To mitigate cybersecurity risks associated with 5G networks, the EU in 2020 advanced the "Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures.” The Toolbox provides essential guidance to stakeholders and actors across the 5G supply chain. Additional measures supporting the exchange of user experiences from “in the field”, using the toolbox, could support the improvement of the Toolbox or development of further guidance.

At present, clusters and innovation networks are only just establishing. Of note is the 5G Infrastructure Public Private Partnership (5G PPP), a joint initiative among the European Commission and European ICT industry (including manufacturers, telecommunications operators, service providers, SMEs and research institutions). Recognizing a trend toward private 5G networks, expanding support for regional clusters—including verticals using 5G networks—would also be important for system-wide integration.

A discussion of sector verticals leads us to consider the demand side of 5G technologies and networks. Policies to support private demand for 5G networks have only just started, for example as visible in the German initiative or the common German-French support for private networks. National and multi-national initiatives would benefit from expansion, as well as a more general focus on the demand side at the European level (as suggested by several experts in the second stakeholder workshop of this study).

Complementary to but a potential stimulant for private demand, leveraging public procurement could further accelerate 5G technology and network rollouts. So far security concerns have been in the focus of public procurement related to 5G. However, the potential of public procurement to push not only the public demand for 5G technologies and networks, but demand is the key objective for the near future. Providing the 5G infrastructure will stimulate demand, e.g. by developing new business models also for verticals.

Returning to the question of the supply market, EU-wide certifications and standards would benefit from more robust attention and support. Certification schemes already exist for cybersecurity and could be additionally developed in other areas (e.g., energy efficiency). Clear certifications and standards would help new suppliers or start-ups enter the 5G supply chain. The potential for 5G Open-source standards remains similarly underdeveloped. Experimental approaches to testing equipment networks (e.g., bringing together operators and suppliers), open platforms, or experimental applications could generate critical insights and feedback to further improve

185 Pohlmann et al. (2020)

standardization activities. Putting such experiments into conversation with standardization activities point to the need for integrative EU-wide support schemes in this area. Turning to regulatory frameworks related to 5G networks, the focus so far has been on spectrum issues and cybersecurity risks. These dimensions remain of high relevance to ensure efficient regulation of spectrum, address security concerns and support productive competition. Moving forward, the regulatory focus will need to expand to address energy efficiency issues. Further, calls for digital autonomy require additional regulatory action in the European 5G supply chain to keep a close watch on mergers and acquisitions and price dumping practices. A more comprehensive regulatory approach is needed to address security, sustainability, competition, digital autonomy and supply-side diversity (or robustness) concerns.

In general, there are different ways for stakeholders or policy-makers to use scenarios for strategy development and decision-making.[186] One approach is to develop "proactive strategies" and to focus on those scenarios which can be shaped sufficiently and are in line with political goals. In contrast, the traditional planning approach suggests taking the scenario which is assessed as most likely and developing a strategy in line with this scenario. However, in our case, there is not a clear scenario that can be considered as significantly more likely than the other strategies. Another approach is to develop "preventive strategies", which means to avoid that a specific scenario with a very high risk turns into reality, which is, for instance, used in risk management. In our case, this would mean to prevent that scenario 2 (Slow pace of 5G Roll out) which has been assessed to bear the biggest risks for the European economy as having the becomes reality. A further, more advanced way is to develop "adaptive strategies" which can cope with more than one strategy and leave some flexibility to respond to changing conditions in the future. Such strategies or policies are more robust and help with navigating today's complex economic, social and political environment. This is the approach that offers a robust strategy to deal with the different opportunities and risks of the different strategies. It is advocated to adopt this approach to exploit the opportunities of scenarios I, III and IV and avoid its risks at the same time.

However, for each of the four scenarios presented, critical future policy measures can be deduced to support robust 5G ecosystem development:

- In Scenario I, where incumbent players drive 5G, competition policy would do well to ensure start-ups and new companies can enter the supply side market.
- In Scenario II, characterized by a delayed roll-out of 5G technologies and networks, a focus on demand-side support (e.g., through public procurement, private network, sector verticals, and use cases for development) would be essential. Complementing demand support, additional funding for supply side research and innovation, related to technology vendors and MNOs, would be important.
- In Scenario III, Open RAN evolves into a game-changing development, which might generate novel challenges related to standardisation, network security, and energy efficiency. Consequently, and in response, framework conditions for internationally interoperable and accepted standards would need to be developed. Security and energy efficiency challenges would have to be addressed not only in standardisation but also in certification schemes, and, possibly, even the regulatory frame governing Open RAN.
- Finally, in Scenario IV the competition and industrial policy of the EU—as revealed by previous experiences with Big Tech companies—will be vital. Acquisition of promising EU-based SMEs and start-ups by dominant Big Tech companies in Scenario IV would also necessitate stronger policies for digital sovereignty in the EU. Indeed, Big Tech business models and financial power could even endanger the survival of European MNOs. Furthermore, their proprietary standards, but also their strong influence on Open-source187

186 See Fink et al. (2002)
187 See Blind et al. (2021)

can threaten the very successful open standardisation culture at 3GPP concerning 5G standards in the past.

As the above examples demonstrate, the path of 5G ecosystem development is neither set nor certain. No matter which scenario or a mix of scenarios elements manifest in the future, robust national, regional and European policy measures will be essential to mitigating the risks and realizing the opportunities in the area of 5G supply markets in Europe.

7. References

5G Observatory, 2020, 2nd Stakeholder Workshop of the 5G Observatory on 25 September 2020, hg. v. Commission, E.

5G PPP Automotive WG (2019). Business Feasibility Study for 5G V2X Deployment. Version 2.

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2017, September). 5G security: Analysis of threats and solutions. In 2017 IEEE Conference on Standards for Communications and Networking (CSCN) (pp. 193-199). IEEE.

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2018). Overview of 5G security challenges and solutions. IEEE Communications Standards Magazine, 2(1), 36-43.

Ahokangas, P., Moqaddamerad, S., Matinmikko, M., Abouzeid, A., Atkova, I., Gomes, J. F., & Iivari, M. (2016). Future micro operators business models in 5G. The Business & Management Review, 7(5), 143.

Ajibulu, A., Bradford, J., Chambers, C., Fletcher, S., Karousos, A., Konstantinou, K., Osman, H., Droste, H., Rendon Schneir, J., G., Canto Palancar, R., Sciancalepore, V., Yousaf, Z., Rost, P., & Doll, M. (2017). Deliverable D2.3: Evaluation architecture design and socioeconomic analysis - final report. 5G NORMA project.

Aslan, Y., Kiper, C.E., van den Biggelaar, A.J., Johannsen, U. & Yarovoy, A. (2019). October. Passive cooling of mm-wave active integrated 5G base station antennas using CPU heatsinks. In 2019 16th European Radar Conference (EuRAD) (pp. 121-124). IEEE.

Barclays (2021, 16 February). Open RAN in Europe – what's next? Equity Research.

Barford, J. (2021). The push for OpenRAN: Careful what you wish for. ENDER ANALYSIS(20 April 2021). Retrieved from https://www.endersanalysis.com/reports/push-openran-careful-what-you-wish

Biagi, F.; Pesole, A.; Stancik, J. (2016): Modes of Innovation: Evidence from the Community Innovation Survey; Joint Research Centre EUR 27986 EN; doi:10.2791/297083

Biddle, C. Bradford (2019). Linux Foundation is Eating the World, Journal of Open Law, Technology, & Society, 11(1), pp 57 – 74,

Blind, K. & Böhm (2019). The Relationship Between Open-source Software and Standard Setting, EUR 29867 EN, JRC (Joint Research Centre) Science for Policy Report, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11593-9.

Blind, K. & Gauch, S. (2009). Research and standardisation in nanotechnology: evidence from Germany. The Journal of Technology Transfer 34 (3), 320-342

Blind, K. (2016). The Impact of Regulation on Innovation, in Edler et al. (eds) Handbook of Innovation Policy Impact. Edward Elgar Publishing.

Blind, K.; Böhm, M.; Grzegorzewska, P.; Katz, A.; Muto, S.; Pätsch, S.; Schubert, T. (2021): The impact of Open-source Software and Hardware on technological independence, competitiveness and innovation in the EU economy. Final Study Report. Brussels.

Bonati, L., Polese, M., D'Oro, S., Basagni, S. & Melodia, S. (2020). "Open, Programmable, and Virtualized 5G Networks: State-of-the-Art and the Road Ahead," Computer Networks, vol. 182.

Cabral, L. & Salant, D. (2014). "Evolving technologies and standards regulation," International Journal of Industrial Organization, vol. 36(C), 48-56.

Camps-Aragó, P., Delaere, S., & Ballon, P. (2019, September). 5G Business Models: Evolving Mobile Network Operator Roles in New Ecosystems. In 2019 CTTE-FITCE: Smart Cities & Information and Communication Technology (CTTE-FITCE) (pp. 1-6). IEEE.

Checko, A., Christiansen, H.L., Yan, Y., Scolari, L., Kardaras, G., Berger, M.S. & Dittmann, L. (2014). Cloud RAN for mobile networks—A technology overview. IEEE Communications surveys & tutorials, 17(1), pp.405-426.

Chen, Y., Zhang, S., Xu, S. & Li, G.Y. (2011). Fundamental trade-offs on green wireless networks. IEEE Communications Magazine, 49(6), pp.30-37.

Chih-Lin, I., Han, S. & Bian, S. (2020). Energy-efficient 5G for a greener future. Nature Electronics, 3(4), pp.182-184.

Ding, Z., Liu, Y., Choi, J., Sun, Q., Elkashlan, M., Chih-Lin, I. and Poor, H.V. (2017). Application of non-orthogonal multiple access in LTE and 5G networks. IEEE Communications Magazine, 55(2), pp.185-191.

Edler, J. & J. Fagerberg (2017). Innovation policy: what, why, and how, Oxford Review of Economic Policy 33 (1), 2-23.

Edler, J.; Blind, K.; Frietsch, R.; Kimpeler, S.; Kroll, H.; Lerch, C. et al. (2020): Technology Sovereignty: from demand to concept. Perspectives-Policy Brief.

ENISA. (2021a). Securing EU's Vision on 5G: Cybersecurity Certification. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

ENISA. (2021b). Security in 5G specifications – controls in 3GPP Security Specifications (5G SA). European Union Agency for Cybersecurity.

Ercan, E. M., 2013, Global Warming Potential of a Smartphone: Using Life Cycle Assessment Methodology, Student thesis, Trita-IM-EX < http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-136993 >.

ERT, 2020a, Assessment of 5G Deployment Status in Europe, Brussels.

ERT, 2020b, ERT Position on Regulatory Framework for 5G, Brussels.

European Commission, 2019, Member States publish a report on EU coordinated risk assessment of 5G networks security: Press corner.

European Commission, 2020, 2020 Strategic Foresight Report. Charting the course towards a more resilient Europe.

European Union (ed.) (2020): Strengthening Europe's digital and technological sovereignty -. EU2020. Online available under https://www.eu2020.de/eu2020-en/eu-digitalisation-technology-sovereignty/2352828.

European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union.

Federal Ministry for Economic Affairs and Energy (2020): Emerging stronger from the crisis together For a competitive, innovative and resilient European economy: Priorities of the Federal Ministry for Economic Affairs and Energy for the German Presidency of the Council of the EU

Fink, A., Schlacke, O., Siebe, A. (2002): Erfolg durch Szenario-Management, Prinzipien und Werkzeuge der strategischen Vorausschau, Campus, Frankfurt.

GeSI (2015). #SMARTer2030: ICT Solutions for 21st Century Challenges, Global e-Sustainability Initiative. https://go.nature.com/3ba2ZPA

Grandstrand, O. & M. Holgersson (2020). Innovation ecosystems: A conceptual review and a new definition, Technovation 90, 102098.

GSMA (2018). Enabling Neutral Host. Network Economics: CCS case study.

Hofer, M., 2020, Current Status and Outlook on Open Radio Access Network initiatives, Zenodo.

Huttunen, J., Salmela, O., Volkov, T. & Pongrácz, E. (2020). Reducing the Cooling Energy Consumption of Telecom Sites by Liquid Cooling. In Multidisciplinary Digital Publishing Institute Proceedings (Vol. 58, No. 1, p. 19).

Kastenhofer, K., Mesbahi, Z. & Schaber, F., 2020, 5G-Mobilfunk und Gesundheit, 2020/03/09/, Wien.

Koch, C. & K. Blind (2021). Towards agile standardisation: Testbeds in support of standardisation for the IIoT, IEEE Transactions on Engineering Management 68 (1), 59-74.

Koch, C. & K. Blind (2021): Towards agile standardisation: Testbeds in support of standardisation for the IIoT, IEEE Transactions on Engineering Management 68 (1), 59-74.

Larsson, E.G., Edfors, O., Tufvesson, F. & Marzetta, T.L. (2014). Massive MIMO for next generation wireless systems. IEEE communications magazine, 52(2), pp.186-195.

López-Pérez, D., De Domenico, A., Piovesan, N., Baohongqiang, H., Xinli, G., Qitao, S., & Debbah, M. (2021). A survey on 5G energy efficiency: massive MIMO, lean carrier design, sleep modes, and machine learning. arXiv preprint arXiv:2101.11246.

McEntaggart, K., Etienne, J., Beaujet, H., Campbell, L., Blind, K., Ahmad, A., Brass, I. (2020): Taxonomy of regulatory types and their impacts on innovation: Final report, BEIS Research Paper, No. 2020/4, UK Government, Department for Business, Energy & Industrial Strategy, London

Moqaddamerad, S., Ahokangas, P., Matinmikko, M. & Rohrbeck, R., 2017, Using Scenario-based Business Modelling to Explore the 5G Telecommunication Market, Journal of Futures Studies, 22(1), 1-18.

Mughees, A., Tahir, M., Sheikh, M.A. & Ahad, A. (2020). Towards Energy Efficient 5G Networks Using Machine Learning: Taxonomy, Research Challenges, and Future Research Directions. IEEE Access, 8, pp.187498-187522.

Nagle, F., Wheeler, D. A., Lifshitz-Assaf, H., Ham, H., & Hoffman, J. L. (2020). Report on the 2020 FOSS Contributor Survey. The Linux Foundation & The Laboratory for Innovation Science at Harvard.

NIS Cooperation Group, 2019, EU coordinated risk assessment of the cybersecurity of 5G networks, im Auftrag von: Commission, E.

Niu, K., Chen, K., Lin, J. & Zhang, Q.T. (2014). Polar codes: Primary concepts and practical decoding algorithms. IEEE Communications Magazine, 52(7), pp.192-203.

O'Halloran, J. (2020). Elisa enjoys 5G base station energy, emissions reductions from Nokia liquid cooling. Computer Weekly. https://www.computerweekly.com/news/252484174/Elisa-enjoys-5G-base-station-energy-emissions-reductions-from-Nokia-liquid-cooling

OECD (2015): System Innovation: Synthesis Report, OECD, Paris.

OECD, 2019, The road to 5G networks.

Oughton, E. J., & Frias, Z. (2018). The cost, coverage and rollout implications of 5G infrastructure in Britain. Telecommunications Policy, 42(8), 636-652.

Oxford Analytica (2021). 5G opportunities carry multiple cybersecurity risks, Expert Briefings. https://doi.org/10.1108/OXAN-DB260370

Pathak, A. & Dhote, T. (2021). Relevance of Cybersecurity in 5G Network. International Journal of Modern Agriculture, 10(2), pp.119-126.

Patrick, M., Robilliard, M., Coles, S. & Gardiner, A. M. (2021). Open RAN in Europe - what's next? Barclays.

Pelkmans, J. (2001) The GSM standard: explaining a success story, Journal of European Public Policy, 8:3, 432-453, DOI: 10.1080/13501760110056059

Peters, M. A. & T. Besley (2019) 5G transformational advanced wireless futures, Educational Philosophy and Theory, DOI: 10.1080/00131857.2019.1684802

Pihkola, H., Hongisto, M., Apilo, O. & Lasanen, M., 2018, Evaluating the Energy Consumption of Mobile Data Transfer—From Technology Development to Consumer Behaviour and Life Cycle Thinking, Sustainability 10(7).

Plantin, J.-C. (2021). The political hijacking of open networking. The case of open radio access network. LSE Research Online Documents on Economics. Retrieved from https://ideas.repec.org/p/ehl/lserod/109858.html

Pohlmann, T., Blind, K. & Heß, P. (2020). Fact finding study on patents declared to the 5G standard. Report on behalf of the German Ministry of Economic Affairs and Technology.

Pujol, F., Manero, C. & Jaffal, T., 2018, 5G Observatory Quarterly Report 2 Up to December 2018, im Auftrag von: European Commission, Directorate-General of Communications Networks und Content & Technology: IDATE Digiworld.

Pujol, F., Manero, C. & Jaffal, T., 2019, 5G Observatory Quarterly Report 4 Up to June 2019, im Auftrag von: European Commission, Directorate-General of Communications Networks und Content & Technology: IDATE Digiworld.

Pujol, F., Manero, C., Carle, B. & Remis, S., 2020a, 5G Observatory Quarterly Report 8 Up to June 2020, im Auftrag von: European Commission, Directorate-General of Communications Networks und Content & Technology, July 2020: IDATE Digiworld.

Pujol, F., Manero, C., Carle, B. & Remis, S., 2020b, 5G Observatory Quarterly Report 9 Up to September 2020, im Auftrag von: European Commission, Directorate-General of Communications Networks und Content & Technology: IDATE Digiworld.

Rinkinen, S. & and V. Harmaakorpi (2019): Business and innovation ecosystems: innovation policy implications, Int. J. Public Policy, Vol. 15, Nos. 3/4, 248-265

Schoemaker, P.J.H. (1995): Scenario Planning: A Tool for Strategic Thinking. Sloan Management Review 36, 25–40.

Shah, Y., Chelvachandran, N., Kendzierskyj, S., Jahankhani, H. & Janoso, R. (2020). 5G Cybersecurity Vulnerabilities with IoT and Smart Societies. In Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity (pp. 159-176). Springer, Cham.

Stolton, S. (2021). EU charts cybersecurity certification scheme for 5G. Euractiv. https://www.euractiv.com/section/5g/news/eu-charts-cybersecurity-certification-scheme-for-5g/

Suomalainen, J., Juhola, A., Shahabuddin, S., Mämmelä, A. & Ahmad, I. (2020). Machine learning threatens 5G security. IEEE Access, 8, pp.190822-190842.

Tăbușcă, A. & Tăbușcă, S.M. (2019). The Impact of 5G Technology in Global Economy, Cybersecurity and Legal Issues. Journal of Information Systems & Operations Management, 13(2).

Taga, K., Uferer, C. & McInroy, C. (2021). 5G Supply Market Trends: Baseline Scenario Report.

Teece, D. J. (2018). Profiting from innovation in the digital economy: Enabling technologies, standards, and licensing models in the wireless world. Research Policy, 47(8), 1367-1387.

Teubner, L.K., Henkel, J. & Bekkers, R. (2021) Industry consortia in mobile telecommunications standards setting: Purpose, organization and diversity, Telecommunications Policy, Volume 45, Issue 3.

Timmers, P. (2019). Ethics of AI and cybersecurity when sovereignty is at stake. Minds and Machines, 29(4), pp.635-645.

Usama, M. & Erol-Kantarci, M. (2019). A survey on recent trends and open issues in energy efficiency of 5G. Sensors, 19(14), p.3126.

Uyarra, E., and Ramlogan, R. (2016), ‘The Impact of Cluster Policy on Innovation’, in J. Edler, P. Cunningham, A. Gök, and P. Shapira (eds), Handbook of Innovation Policy Impact, Cheltenham, Edward Elgar, 279–317.

Von Laer, M., Blind, K. & Ramel, F. (2021): Standard essential patents and global ICT value chains with a focus on the catching-up of China, Telecommunications Policy, DOI: 10.1016/j.telpol.2021.102110

Wheeler, T. & Simpson, D. (2019): Why 5G requires new approaches to cybersecurity. Racing to protect the most important network of the 21st century. Brookings. https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity

World Economic Forum, 2020, The Global Risks Report 2020: World Economic Forum.

Zhang, S., Xu, X., Wu, Y. & Lu, L. (2014): 5G: Towards energy-efficient, low-latency and high-reliable communications networks. In 2014 IEEE international conference on communication systems (pp. 197-201). IEEE.

Zhang, X., Kunz, A., & Schröder, S. (2017, September). Overview of 5G security in 3GPP. In 2017 IEEE conference on standards for communications and networking (CSCN) (pp. 181-186). IEEE.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

KK-05-21-235-EN-N

Publications Office of the European Union

doi: 10.2759/017326
ISBN 978-92-76-40349-4