cerre Centre on Regulation in Europe

THE FUTURE OF EUROPEAN TELECOMMUNICATIONS: IN-DEPTH ANALYSIS

RICHARD FEASEY
ALEXANDRE DE STREEL
PETER ALEXIADIS
MARC BOURREAU
MARTIN CAVE
ILSA GODLOVITCH
ANTONIO MANGANELLI
GIORGIO MONTI
TONY SHORTALL
PAUL TIMMERS

September 2024

cerre

Report

The Future of European Telecommunications: In-depth Analysis

Richard Feasey
Alexandre de Streel
Peter Alexiadis
Marc Bourreau
Martin Cave
Ilsa Godlovitch
Antonio Manganelli
Giorgio Monti
Tony Shortall
Paul Timmers

September 2024

As provided for in CERRE's bylaws and procedural rules from its "Transparency & Independence Policy", all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: ARCEP, Agcom, BIPT, Comreg, Amazon, Deutsche Telekom, Huawei, Microsoft, Ofcom, Orange, Qualcomm, Telecom Italia. However, the views, opinions and conclusions expressed in this report are solely those of the authors in a personal capacity. They do not necessarily reflect the position of, and cannot be attributed to any of the abovementioned organisations. Neither these, nor any institution with which the authors are associated, nor any other member of CERRE, nor CERRE itself bear any responsibility for the content of the report or necessarily endorse it.

info@cerre.eu – www.cerre.eu

Table of Contents

About CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

About the Authors

Richard Feasey is a CERRE Senior Adviser, an Inquiry Chair at the UK's Competition and Markets Authority and Member of the National Infrastructure Commission for Wales. He lectures at University College and Kings College London and the Judge Business School. He has previously been an adviser to the UK Payments Systems Regulator, the House of Lords EU Sub-Committee and to various international legal and economic advisory firms. He was Director of Public Policy for Vodafone plc between 2001 and 2013.

Alexandre de Streel is the Academic Director of the digital research programme at CERRE and Professor of European law at the University of Namur where he chairs the Namur Digital Institute (NADI). Alexandre is also visiting professor at the College of Europe (Bruges) and SciencesPo Paris. Besides, he chairs the expert group on the online platform economy advising the European Commission and is a part-time judge at the Belgian Competition Authority. His main areas of research are regulation and competition policy in the digital economy as well as the legal issues raised by the developments of artificial intelligence.

Peter Alexiadis is a Visiting Professor at King's College, where he teaches the LLM modules on 'Competition Law & Regulated Network Sectors' and 'Digital Regulation'. He is also a Research Fellow at CERRE. Peter was a competition law and regulatory policy specialist attorney in Brussels for well over three decades, where he was recommended as a leading attorney in both areas of practice by all peer reviews. He has acted as an external adviser to the European Commission's DG Competition Telecommunications Unit, and has played a very active role in the crafting of the existing regulatory frameworks for electronic communications and digital platforms.

Marc Bourreau is an Academic Co-Director at CERRE and Professor of Economics at Télécom Paris (Institut Polytechnique de Paris). He is affiliated with the interdisciplinary institute for innovation (i3) for his research. His research focuses on competition policy and regulation, digital markets, and telecommunications. Marc holds a Ph.D. in Economics from the University of Paris Panthéon Assas.

Martin Cave is a Visiting Professor at Imperial College London. He was an Academic Co-Director at CERRE. He is a regulatory economist specialising in competition law and in the network industries, including airports, broadcasting, energy, posts, railways, telecommunications and water. Professor Cave has published extensively in these fields, and has held professorial positions at Warwick Business School, University of Warwick, and the Department of Economics, Brunel University.

Ilsa Godlovitch is an expert on telecoms and the digital economy with more than 20 years of experience in managing and conducting research and regulatory projects in this field. Ilsa has led studies for the European Commission regarding the Gigabit Infrastructure Act, Open Internet and Roaming Regulations, EU Electronic Communications Code and Broadband State Aid Guidelines, as well as conducting research for BEREC and National Regulatory Authorities on the environmental impact of electronic communications, and the evolution of fixed and mobile telecom markets.

Antonio Manganelli is Professor of Antitrust and Regulation at the University of Rome LUMSA, where he is also programme coordinator for the M.Sc. in Antitrust, Regulation and Innovative industries. Antonio holds a Ph.D. in Law and Economics from the University of Siena. He previously worked as Research Associate at the European University Institute, as coordinator of the Florence School of Regulation, and in several public institutions.

Giorgio Monti is a Professor of Competition Law at Tilburg Law School. He began his career in the UK (Leicester 1993-2001 and London School of Economics (2001-2010) before taking up the Chair in competition law at the European University Institute in Florence, Italy (2010-2019). While at the EUI he helped establish the Florence Competition Program which carries out research and training for judges and executives. He also served as Head of the Law Department at the EUI. His principal field of research is competition law, a subject he enjoys tackling from an economic and a policy perspective.

Tony Shortall is a Director of Telage, a Brussels-based consultancy firm in the field of telecommunications economics and regulation. He is an economist specialising in the regulation of network industries and has written extensively on these matters and has advised governments, regulators and firms.

Prof Dr Paul Timmers is a research associate at the University of Oxford, Oxford Internet Institute, professor at European University Cyprus, visiting professor at KU Leuven and the University of Rijeka, senior advisor EPC Brussels, President of the Supervisory Board Estonian eGovernance Academy and CEO of iivii. Previously, he was Director at the European Commission/DG CONNECT where has held responsibility for legislation and funding programmes for cybersecurity, eID, digital privacy, digital health, smart cities, and e-government. At the European Commission, he was also a cabinet member of European Commissioner Liikanen. He worked as manager of a software department in a large ICT company and co-founded an ICT start-up.

Executive Summary

The issue papers in this report supported the analysis for the "Ideas for the Future of European Telecommunications Regulations" publication. The resulting recommendations are outlined in the executive summary below.

- The current telecoms regulatory framework was introduced in 2002. It has proved flexible in accommodating a number of major changes in the structure of the industry (end of the State-owned monopolists), technology (broadband and mobile internet) and political objectives (more focus on investment in new technologies and less on price). However, after more than 20 years of existence, the European Commission is right to ask whether the telecoms regulatory framework is still appropriate for the future.
- Asymmetric economic regulation in telecoms has reduced as competition has increased, as was originally intended (the number of markets under the Significant Market Power (SMP) regime has reduced from 18 to 2 since 2002). But symmetric regulation has increased, and new and sometimes unexpected regulations have also been added outside the SMP regime: to reduce roaming fees and international call charges, to give access to ducts and poles, to ensure an 'open internet' and require removal of Chinese equipment on security grounds. These have reflected new political objectives for the telecoms sector, including increased focus on security, resilience or sustainability and single market goals.
- For mobile operators, these unexpected forms of regulation – and the cost of spectrum – have had a bigger effect than SMP regulation, which is much more significant for fixed operators. The impact of different types of regulation is therefore different for each activity.
- The existing regulatory regime aims to promote competition and has been quite successful at this, particularly for new fibre networks where Europe is more competitive than the US or other regions. The EC should be paying more attention to measuring competition alongside coverage. This is challenging because many fibre networks are local rather than national and infrastructure competition differs a lot between urban and rural areas. The industry and the landscape is more complex and fragmented now than in the past and future regulation needs to be able to handle this.
- Competition in mobile is more stable and is similar in Europe to the rest of the world, with 3-4 operators in most markets. On the basis of the data we looked at, the differences between Europe and the rest of the world on mobile, including 5G, do not seem to be mostly explained by differences in market structure.
- There are significant differences (up to 4x) between Member States if we look at the prices, network coverage and use of telecoms services, including fibre and 5G. These differences are often bigger than any differences between the EU and other regions of the world. They don't seem to be reducing, and it is not yet clear why they arise within the same regulatory framework.

- The same applies to the financial performance of different European telecoms operators, some of whom earn better returns and have lower financing costs than others. In general, the financial performance of the European industry has deteriorated to a greater extent than in the US or other regions. The outlook in Europe for the future is uncertain. This points to the need for the EC to take a cautious approach to regulation and target setting in future.
- Compared to most of the rest of the world including the US and Japan, some European Member States or operators are performing well on fibre (Spain, France) or 5G (Italy with Wind, Finland with Telia) or both (Netherlands), while others are lagging behind. 5G 'coverage' is particularly difficult to measure or compare, and the EC should improve its ability to do so. Given these wide variations, we should be cautious in using a European 'average' performance to compare with other regions.
- Some argue that Europe would have better performance if operators were 'pan European' and had more subscribers. There is, however, limited evidence at this stage inside Europe or when comparing with other regions that the number of subscribers determines profitability or how well operators perform. Fixed broadband prices are lower and fibre coverage is higher in Hungary than in Italy. Mobile prices are lower and 5G coverage higher in Denmark and Finland than in Germany. Large European operators have more fibre customers than US operators, and similar numbers of mobile customers. The industry structure will be determined by the owners of those firms, who will respond to economic and commercial opportunities, and not by the EC.
- Changes in the wider digital economy as well as changes in the technology used by telecommunications operators themselves (including increasing reliance on cloud services) could have far reaching consequences in the future.

Recommendations

- Significant Market Power (or SMP) regulation was designed when fixed telecoms markets were dominated by former State-owned national monopoly networks. It has enabled competition to develop and allowed regulation to be withdrawn as it does. SMP regulation may still be required in future but the landscape it applies to will be different going forward: market power will be more localised and may exist when more than one operator is present (e.g. in a duopoly). SMP regulation may not be so effective in these circumstances, may distort competition or may be applied less consistently as it becomes more complex. We recommend that the European Commission considers an alternative, better tailored, approach which targets 'bottlenecks' instead of SMP. This would focus on the assets to which access is required to compete rather than the position of the owner of the assets. Making this change would present some challenges in terms of legal certainty in the short term. The alternative is to tighten and improve the way the existing SMP regulation is applied, for example by requiring national regulators to prove that a particular telecom market justifies intervention next to competition law in order to preserve the users' long-term interests.

- We support the rapid retirement of copper networks to avoid wasteful duplication but do not think that EU compulsory targets are needed to achieve this. One key issue is whether an owner of a copper network must retire it if the alternative fibre network that is available is owned by a competitor or only when it has a network of its own available. If the former, the copper network owner may require some form of compensation. Whilst copper networks are still in use, we think more public subsidies should be used to encourage users to switch to fibre.
- Whether spectrum policies in Europe have worked well in the past or not is less important than a policy that is suitable for the future. With less new spectrum to auction, the main aim should be to avoid spectrum regulation imposing unexpected costs for the industry and ensure that already available spectrum is being used efficiently. The quid pro quo we recommend is that operators are given longer term spectrum licences at no charge, but in return become subject to a 'use it or lose it' obligation which involves national regulators monitoring how well the spectrum is used. Regulators will need to change their approach in order to implement and enforce this approach properly and will need legal powers to do so.
- We do not recommend fundamental changes in competition law, but the EU merger regime may take a more dynamic approach to efficiency and consumer welfare. The facts which the EC needs to take into account should also reflect the changes in the industry. Network and other sharing arrangements could become easier to approve as control of networks moves to the cloud. More account should be taken of the security, resilience and sustainability implications of mergers and horizontal agreements, although these objectives may pull in different directions.
- As most Europeans are now accustomed to having competitive telecoms markets, some of the telecom-specific consumer protection regulation could be phased out; we could rely more on general rules that apply in the wider economy. Users and regulators have tended to focus on getting the lowest price in the past, but effort should now be made to focus as much or more on quality.
- There is a risk that the current interpretation of the Open Internet Regulation could prevent operators from offering distinctive 5G services, undermining the other EC objectives for 5G. The EC should be mindful of those risks and possibly adapt EU law and/or its interpretation.
- The approach to 'universal service' in Europe needs fundamental rethinking after years of piecemeal changes and additions. Are we concerned that low-income households can access telecoms services which the rest of us already have or are we using subsidies to promote widespread adoption of new leading edge technologies by everyone? How do these objectives relate to the public subsidies given to operators to extend their networks or to replace Chinese equipment or retire copper networks early? Addressing these questions in a coherent way will require a new approach to the use of public subsidies in the telecoms industry and new mechanisms for distributing funds.

- It seems clear that the European telecoms industry will need to invest more in security and resilience in the future. Again, we need to see a more strategic and aligned approach from the EC and Member States, anticipating developments before they happen and providing public funds where necessary, rather than imposing unbudgeted costs on operators, as when requiring the removal of Chinese equipment from 5G networks after it had been installed. We should aim to improve security without compromising competition in telecoms or our ability to collaborate with other regions to develop new technologies.
- The EC's aims of expanding network coverage and increasing adoption and use of new 5G devices have significant environmental trade-offs which need to be recognised and mitigated. Users would be encouraged to better consider the environmental costs of using different digital services if operators were required to provide required real-time information about the network resources they consumed. Operators could be required to report on the environmental impacts of networks by reference to a set of standard measures or targets which should be developed by the EC itself.
- Many of the other recommendations featured in this CERRE report – to retire copper networks, allow operators to better manage their networks under the Open Internet Regulation and enable greater network sharing – also ought to contribute to efficiency and sustainability goals. The European Commission should revisit some of its targets and consider alternative technologies in light of the environmental as well as the economic costs involved in deploying fibre or 5G networks in very remote areas.

cerre Centre on Regulation in Europe

MARKET AND ECONOMIC REGULATION

PETER ALEXIADIS
ALEXANDRE DE STREEL

1. Introduction

In this first in a series of issue papers, we have formulated a number of proposals for changes to the existing EU regulatory framework for electronic communications that came into effect in 2002 and which has most recently been amended in 2018 with the adoption of the *European Electronic* Communications Code (*EECC*).[1] To this end, we foresee that the following important balancing exercises should instruct policy makers in their decision-making, namely:

- Conceding that the pursuit of multiple **policy goals** in terms of competition, sustainability, pricing, investment, innovation, network integrity and security, can generate tensions and will inevitably compromise the pursuit of certain policy goals in favour of others.
- Identifying the **structure of markets** and shifts in the nature of the **value chain** in digital markets driven by technology, insofar as these characteristics accommodate certain types of policy intervention.
- Identifying the most appropriate and coherent combination of **public money and private investment** – both from an *ex-ante* and an *ex-poste* perspective - that should be devoted to achieving key policy aims, especially when taking into account how other sectoral regimes balance such a process.
- Acknowledging that the commitment to fostering an **internal market** for connectivity needs to take due account of realistic commercial and technical reasons that perpetuate national markets.
- Exploring the level and type of **complementarity** that should be pursued between the application of *ex-ante* and *ex-poste* rules.

Based on the review of current state of technological development and their likely impact on business models and investment incentives, our analysis of the effectiveness of current regulatory policy in the EU affecting connectivity suggests that various lines of enquiry should be pursued that are directed at the revisiting regulatory obligations under the *EECC*, consistent with what was originally foreshadowed in the EU Regulatory Framework of 2002.

A lack of consumer demand for high-bandwidth fixed broadband services and the failure of 5G technology to be the anticipated "game-changer" in terms of its capabilities are but two of a number of factors that are challenging the ongoing ability of connectivity providers to continue their investment momentum.

In addition, connectivity providers are arguably also facing a series of **next generation investment challenges** which include their ability to: (i) provide new innovative services otherwise made possible by recent technological changes; (ii) take advantage of the opportunities afforded under various interoperability and access obligations imposed on 'gatekeepers' under the *Digital Markets Act (DMA)*; and (iii) exploit the scale necessary to provide cross-market IoT services. These challenges in services need to be supported by accompanying investments in infrastructure beyond the high levels

[1] Directive (EU) 2018/1972, OJ. L 321, 17.012.2018, pp.36-214.

of investment already being expended by existing market actors, which will in turn require outlays in capital expenditure that are prone to uncertain levels of return.

The challenge for policy makers therefore becomes one of how best to identify an appropriate and proportionate regulatory path that can provide the commercial impetus to connectivity providers to engage in these key areas of next generation investment. It is equally important, however, that the positive outcomes for **consumers** delivered under the *EECC* and its predecessors, not be compromised by the onset of identified technological and market developments which would raise the risk of re-monopolisation. This would afford policy makers the freedom to **lower regulatory burdens**, as opposed to other sectors of the economy that are subject to regulation such as energy, where the pattern has been for regulation to intensify over time in response to unsatisfactory market outcomes.

Based on the above considerations, we put forward a **list of potential policy measures that should be considered by policy makers in the short to medium term, with a view to sustaining a stable and robust regulatory environment for connectivity providers for the next twenty years**. Realistically, given the usual political cycle for the introduction, consultation and proposal of EU law, a majority of the measures (other than those recommending the issue of guidance or the interpretation of competition policy) considered for implementation into national law will need to be contemplated.

Where necessary, we have opted for a range of policy options to be considered, especially given the various elements that impact upon decision-making. Otherwise, where we consider that the policy option is more clear-cut, we have opted for Preliminary Recommendations from the outset. The regulatory policy proposals set forth herein, while taking note of the views expressed by the European Commission's *White Paper* '*How to master Europe's digital infrastructure needs?*'[2] which was released on 21 February 2024, should not be seen to be a contribution to the public consultation on that *White Paper,* but as a stand-alone study.

[2] Refer to COM (2024) 81/2.

2. Access Regulation

At the heart of any decision for market intervention will be the issue of which entities fall within the scope of any intended *ex-ante* regulation. The combined effect of changes in technological developments, market dynamics, the natural extension of the digital value chain and the nature of the competitive interactions that occur within it (often described in terms of an 'ecosystem'), alongside regulatory developments in other related areas, challenge whether the thresholds or triggers used for over twenty years to justify the imposition of *ex-ante* regulatory obligations on connectivity providers should change.[3]

2.1 Possible limits of the current SMP regime

2.1.1. Market definition

Since 2002, regulation in the electronic communications sector has been based on the understanding that a screening test should be performed in advance of two distinct analytical steps are taken to support a decision to impose economic (asymmetric) regulation on operators, based on a list of remedies specified in the *Access Directive* (and more recently in the *EECC*). The screening of potential designated relevant "**markets**", as understood in antitrust terms, occurs by reference to the so-called "**three criteria test**".[4] The first clear analytical step to be performed is that which requires relevant markets affected by potential regulatory intervention to be delineated with precision in accordance with traditional competition law principles. Thereafter, the second analytical step requires that a regulated operator or operators that are active in the designated relevant market be subject to regulatory obligations if they are designated as having "Significant Market Power "(SMP) in the relevant market that has already been delineated.[5]

The question which needs to be asked is whether the positive economic indicators relating to numbers of competitive options, prices and quality, coupled with the challenges faced by operators in sustaining current levels of investment in the *future,* are sufficient to justify a change in the regulatory test in relation to connectivity relationships.

While it is arguable that some variant of the "three criteria test" screening mechanism should continue to be in place to serve as the rationale for regulation in order to ensure that regulatory intervention is appropriate and proportionate (consistent with the principle of good administration), we also need to ask whether the process of market definition should continue to be maintained in its current form, given the existence of the following considerations:

[3] This Section focuses on asymmetric economic regulation, which subjects individual operators to positive and negative obligations *vis a vis* their competitors in order to prevent their market foreclosure. Symmetric obligations involve reciprocal obligations imposed on all markets actors, based on the understanding that the widespread availability of such conduct is essential for the interconnectedness of the sector and/or for the pursuit of broader policy goals and for the benefit of all consumers. Any proposed change in regulation for asymmetric obligations does not necessarily mean that there will be a comparable easing of symmetric obligations.

[4] Namely, the cumulative satisfaction of three screening conditions, constituted by: (1) the existence of high and non-transient entry barriers; (2) the failure of sustainable competition to emerge behind the identified entry barriers; and (3) the inability of competition law to address the likely competitive problems that would arise in the absence of regulation.

[5] A. de Streel, 'The Integration of Competition Law Principles in the New European Regulatory Framework for Electronic Communications', *World Competition* 26(3), 2003, 489-514.

First, the fact that a **very small number of designated markets** (two fixed line markets, down from the original 18 recommended markets specified in 2002) that now satisfy the "three criteria" test at EU level means that the basis of asymmetric regulation under the *EECC* may be disproportionately skewed to cater for them. The shift in regulatory focus for certain markets from asymmetric to symmetric regulation (*e.g.*, termination rates) or to *sui generis* regulation (*e.g.*, international roaming) provides examples of services that can arguably be accommodated under a different format than that of market definition. Moreover, the direction of the EU Regulatory Framework has from the outset been directed towards de-regulation and reliance on the exercise of competition policy once markets are found to be competitive at the retail level. The public policy necessity in defining wholesale 'markets' that attract asymmetric economic regulation also breaks down to some degree if the competitive conditions identified at retail level yield positive economic results. A counterweight to this argument is the fact that a number of Member States continue to regulate specific recommended 'markets' that continue to satisfy the "three criteria" test, irrespective of whether they continue to be specified in the latest version of the EU's *Relevant Markets Recommendation*.

Second, while it is a wholly legitimate exercise for NRAs to define infrastructure-based markets on a sub-national (*e.g.*, regional or local) basis to reflect the local competitive conditions under which they operate, this common practice of **identifying sub-national markets** has had the effect of further fragmenting the EU and challenging operators that wish to provide seamless cross-border services. Segmentation is especially prevalent in those regions where cable TV networks provide a viable alternative to traditional PSTN networks or where Member States reflect unique "*highlands and islands*" geographic characteristics. In the same vein, the prevailing tendency of NRAs increasingly to **differentiate their remedies** within a delineated market has also challenged the harmonisation goal, as in practice it creates a patchwork of remedies across a Member State. The counterweight to this argument is that the importance of achieving targeted regulation at local level should arguably be more of a public policy priority than the pursuit of the internal market goal. In addition, in various jurisdictions the identification of sub-national markets or the use of differentiated remedies in certain Member States has taken place in pursuit of a de-regulatory policy.

Third, it is also the case that the **maintenance of existing *ex-ante* access obligations imposed in the territories of a number of Member States on the basis of market analysis under the existing EU Regulatory Framework has become less necessary over time**, given that:

- symmetric regulation has been increased and strengthened over the years;
- access remedies and other behavioural remedies have already been imposed in the context of many fixed line merger control reviews in the sector;
- the access obligations imposed on MNOs as part of the authorisation/licensing of every new generation of mobile technology has created additional access options; and
- the access obligations which are imposed as a condition of grant of State aid under the *Broadband State Aid Guidelines* has created conditions for third party access in certain geographic areas (usually rural), without dependence on access being provided by a vertically integrated operator.

In addition, most connectivity providers participate in **market structures which are characterised by complex oligopolies**, often consisting of 3-4 providers of mobile services in each Member State and

more of a patchwork of smaller numbers of fixed network providers. Given the inherent difficulties of establishing a finding of collective dominance (or joint-SMP) in mobile markets and the increasingly difficult exercise of identifying individual dominance in those fixed broadband markets that are characterised by relatively competitive retail markets, perhaps the utility of relying on the definition of 'markets' is less viable as an effective basis for future regulatory intervention on a pan-European basis.

Finally, the most recent tendency in the Commission's merger review practice (*e.g.*, the *Booking/Traveli* case, among other digital platform merger cases) and the publication of the *Market Definition Notice* in February 2024 confirm that the Commission is willing, in appropriate circumstances, to assimilate the notion of an '**ecosystem'** with that of an antitrust 'market' when identifying likely market failures or potential market abuses in complex digital environments.[6] This reinforces the view that it is market power and its potential to be exercised that lie at the heart of antitrust analysis and merger control practice, rather than an over-reliance on the initial analytical step of market definition.

Assuming that these alternative bases for regulation are respected in practice by operators, **the collective impact of these trends might mean that it may be less compelling for many operators to be subject to asymmetric access regimes which are based on the identification of antitrust 'markets'**. The working premise must, however, be that the enforcement of other relevant obligations must nevertheless be effective in practice, both in terms of compliance history and institutional design used to administer such obligations.

In addition, perhaps a more holistic view of anticipated harm absent regulation is justified to take into account the essential subject-matter of connectivity, on the one hand, and services delivered through digital platforms, on the other.[7] On the understanding that both of these types of service arguably now fall within the scope of a broader **'ecosystem' of digital communications**, a greater convergence in approach may be desirable if the digital value chain now incorporates both functions. In the case of the Cloud, for example, given that certain aspects of its operation might equally be considered to fall under either of the existing regulatory regimes under the *DMA* and the *EECC*, the adoption of a coherent approach which explains the delineation points between those regulatory regimes, and how they interact with one another, appears to be desirable.[8] The lack of coherence in approach is best reflected in the fact that the *DMA* excludes expressly from its scope electronic communications, yet both the *DMA* (Article 7) and the *EECC* (Article 2(4)) both address some of their provisions to "*number-independent interpersonal communication services*".

All this suggests that **there may be limits to the application of the market definition concept *stricto sensu* in the broader context of digital value chains**. Moreover, a new strand of antitrust economic literature is emphasising the importance of market power analysis (especially in relation to more complex innovative markets) without the need to undertake the preliminary analytical step of market

[6] Commission Notice on the definition of the relevant market for the purposes of Union competition law [2024] OJ C/2024/1645, para 104.

[7] The adoption of a more holistic approach also takes into account matters that go beyond direct consumer harm, including legitimate public interest concerns such as resilience, economic security, environmental sustainability, and the lack of interoperability, all of which can lead to anti-competitive market outcomes.

[8] However, the *DMA* might not be the best framework to regulate Cloud. In this regard, see Manganelli and Schnurr, "*Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies*" (CERRE, 2024).

definition.[9] Accordingly, it is arguable that, based on a forward-looking approach, any review of the current EU Regulatory Framework should consider the utility of such an approach in relation to connectivity relationships.

2.1.2. Significant Market Power

Any re-assessment of the process of market definition should occur in parallel with any re-assessment that might occur in relation to the concept of market power, given that both elements form part of an integrated approach towards asymmetric regulation under the existing SMP regulatory framework. In this regard, **consideration might be given to whether a regulatory trigger could consist of an amalgam between market definition and market power concepts, comparable to the role played by the essential facilities doctrine**. Commentators such as Hellwig have long argued that regulatory intervention should opt for a more holistic approach than applying narrow notions of affected 'markets'. The adoption of such an alternative approach should not mean, however, that the regulatory assessment should be broadened to such a degree as to render it arbitrary in its application.[10]

The adoption of a **more holistic approach**, which considers that likely competitive impacts flow from the control of critical assets which imbue market power, arguably also allows policy makers to take due account of both sides of the broader digital ecosystem, which involves as many aspects of partnering or cooperation as it does of antagonism and challenge among its participants.

From a technological point of view, the progress of key developments such as 'virtualization' and 'softwarization', among others**, may also be having the effect of shifting key economic power away from the centre of the network to its periphery**. Virtualization is actively being pursued by connectivity providers to reduce their costs, while retaining control and ownership of their network assets (although this process is occurring at a relatively modest rate today). However, it also exposes them to the risks of dis-intermediation from their downstream operations. These changes expand the commercial possibilities available to network providers for the provision of advanced communications services. Whether or not operators can effectively manage the provision of such services is, however, problematic. At the same time, taking full advantage of the process of 'cloudification' (insofar as the public Cloud is concerned) is something that connectivity providers are more reluctant to do in the public Cloud (as opposed to their own self-supplied Cloud services) because of their security concerns relating to the migration of their core network intelligence functions and their Radio Access Network. If confirmed, the cumulative effect of these technological changes may be to affect the economic incentives and ability of dominant network operators to exercise market power vis-à-vis other market players.

Given that both antitrust investigations and regulatory interventions under a market analysis approach are driven by the identification of theories of harm - which are in turn based on presumptions about the likely exercise of market power based on the existence of economic incentives or market capabilities - it is therefore **relevant to take these technological changes into**

[9] The influential Cremer Report on the Competition Policy for the Digital era for the European Commission notes at p.3 that: '*in digital markets, we should put less emphasis on analysis of market definition, and more emphasis on theories of harm and identification of anti-competitive strategies*'.

[10] M. Hellwig (2009), "Competition Policy and sector-specific regulation in network industries", in Vives, *Competition Policy: Fifty Years on from the Treaty of Rome.*

account when determining whether or not asymmetric regulation or competition law interventions under Articles 101-102 TFEU is appropriate. In this regard, it is not unreasonable to conceive that a regulatory threshold based on the identification of "Significant Market Power" under the *EECC* might be replaced by a new market power threshold in which such a potential change in economic incentives can be accommodated.

2.2 Adapting the 'bottleneck' concept to changed circumstances

The proposal being considered on the basis of the above observations is, comparable to the principles contained in the 2002 Directives, falls into the category of 'pro-competition regulation' but is designed to take into account the sector's competitive successes witnessed over the past two decades. It is therefore worth **considering replacing the previously borrowed concept of dominance (transposed from competition law as 'SMP' but without an attached theory of harm test) with a new concept that is used elsewhere in competition law - namely, that of an 'adjusted' essential facility doctrine, which we refer to as a 'bottleneck'**.[11] This would constitute a change in terms of the breadth of application of regulation. In an extended value chain, 'bottlenecks' may pop up in unexpected places (as they did, for example, in relation to electronic TV programme guides). It might also more accurately apply to functions such as call termination, rather than reviewing such functions through the prism of a market definition test. Equally, certain types of bottlenecks may emerge in digital markets and involve whole 'ecosystems'.[12]

The concept of a 'bottleneck' is an example of a wider class of *loci* in systems that can be used to exercise power. Other examples include access hubs and centralized oversight operations. Exercising power is often appropriate and necessary to ensure efficient business operation or to safeguard public interests such as resilience, safety, security and environmental sustainability. It can, however, also reflect a potential undue exercise of power or even an abuse of power (*e.g.*, overreach in collecting customer data, anti-competitive behaviour such as that of a gatekeeper). From the perspective of Member States, these control *loci* can be weaponized. [13] The sort of bottleneck that would reasonably fall within the ambit of asymmetric economic regulation is considered in greater detail below.

To the extent that the traditional notion of dominance is deemed to no longer serve as the basis for asymmetric regulation for connectivity providers, the **establishment of a comparable or analogous regulatory threshold to that played by the 'gatekeeper' function** under the *DMA* (a party that manages or contains traffic flows strategically through its positioning in the value chain that allows it to set the conditions of access for third parties) should be considered. Such an approach would be **consistent with the extension of the digital value chain to bring into closer proximity connectivity**

[11] On the relationship between bottleneck and gatekeeper, see A. de Streel, *Gatekeeper Power in the Digital Economy: An Emerging Concept in EU Law*, Note for the OECD, DAF/COMP/WD (2022)57, June 2022.

[12] In the 5 August 2024 *USA v Google LLC* Judgment of District Judge Mehta, Washington DC Circuit (Case No. 20-cv3010, APM) holding Google to have breached Section 2 of the Sherman Act in the field of search, for example, the observation was made that Google controlled a number of "chokepoints" within the ecosystem that it controlled. Such a concept has common origins with the idea that a firm might control a 'bottleneck'.

[13] A bottleneck then becomes a chokepoint, access provision can become problematic, and centralized control can become comprehensive surveillance. While the discussion that follows is focused on bottlenecks in relation to the provision of connectivity services, regulators need to keep in mind that*, mutatis mutandis*, this discussion is also potentially relevant in handling a wider class of control *loci*.

providers with digital platforms and would reflect the interdependence of those parts of the value chain.

Achieving a level of analytical consistency could therefore arguably take the form of adoption of a related **regulatory standard such as a 'bottleneck'** where **access to physical infrastructure or customers** (as in the case of call termination services) is involved. To this end, a bottleneck would be constituted by the existence of a firm with a critical structural position in the production process that is capable of limiting the rate of outflow because of that positioning, thereby causing production delays and raising production costs for competitors.

Because such a proposed legal standard would not have the benefit of drawing upon existing EU case-law, in contrast to the distinctive market definition and market power analyses conducted under the SMP regulatory framework, the definition of a bottleneck would **require careful legislative specification** (as opposed to reliance primarily on 'soft law' clarification, as is the case under the SMP regime) which could hopefully better withstand litigation that challenges its scope of operation. This type of risk is manageable in a number of ways. *First*, by **combining both qualitative and qualitative elements in a working definition**, the scope of the concept becomes less prone to legal uncertainty. To this end, it will be important to set quantitative targets that need to be satisfied and, if departed from, will need to be justified. *Second*, by **crafting an institutional model that administers its key elements** through a more integrated executive approach that is subject to appeals to the European Court, the opportunities for legal uncertainty are diminished as they are subject to one line of legal challenge, rather than 27 different Member State routes (as is currently the situation under the SMP regime).

In this regard, it is worth noting that the preparatory work for the original proposed text of the EU Regulatory Framework in 2002 already considered the adoption of "bottlenecks" as the relevant standard for regulation, as an alternative to the analysis of antitrust "markets".[14] While the bottleneck concept was considered to be one of the definitional options available to the Commission, ultimately the dominance standard was preferred, *inter alia* because that standard was well understood in the antitrust sphere (*i.e.*, because it was subject to European case-law precedent) and because individually dominant firms were clearly identifiable in the fixed line sector (*a contrario* in the expanding mobile communications sector at the time). Moreover, subjecting electronic communications to a market analysis seemed to have merit at the time because the mimicking of market conditions at wholesale level after a period of statutory monopoly created the realistic possibilities for sustainable competition at the retail level. The markets that have emerged post-liberalisation are now mature. Under a 'bottleneck' regulatory standard, the emphasis of policy makers would be to identify situations of strategic control over key resources or customers, as the case may be, that may fall short of traditional ideas of "**essential facilities**" under competition law, while nevertheless reflecting the ability of the relevant operator to be able to exert market power in real terms.

Such a regulatory standard would also **bridge the gap between the identification of a relevant market and a finding of market power**, by treating both of these concepts under a common frame of

[14] See for instance Squire-Sanders-Dempsey and Analysis (1999), *Consumer demand for telecommunications services and the implications of the convergence of fixed and mobile networks for the regulatory framework for a liberalized EU market*, Study for the European Commission; see also P. Larouche (2000), *Competition Law and Regulation in European Telecommunications*, Hart.

reference rather than constituting two distinct analytical steps in the regulatory process. Both standards would also have the potential to be linked or aligned over time to the evolving concept over the next decade of operating within an '**ecosystem'**, which both concepts can accommodate in principle.

The bridging of the digital value chain in this way by reference to two comparable regulatory standards would arguably also **complement any decision over both connectivity providers, on the one hand, and digital platforms, on the other**. At the same time, this type of convergence in regulatory standards would also render arguably more coherent other policy trade-offs that are made between economic stakeholders in different parts of the value chain.

There will no doubt be challenges in defining the concept of a 'bottleneck' in the context of connectivity markets insofar as policy makers only restrict themselves to qualitative criteria, as these may be subject to different emphasis and interpretation. Accordingly, reference to certain **quantitative criteria** should also be considered, including *inter alia* the number of commercially available access options. In addition, the choice needs to be made whether such a standard should be reflected in: (i) individual Decisions of the relevant authority; (ii) specifications under primary legislation (as occurs under the *DMA*); or (iii) in furtherance of guidance provided under a 'soft law' legal instrument (as is the case in relation to market analysis under the *Relevant Markets Recommendation*).

An initial approach as to how to define a bottleneck for *ex-ante* purposes could proceed by **identifying national or sub-national infrastructures or a set of physical or intangible assets (or a combination of both) which provide access to end-user customers.** These identified infrastructures or assets would need to satisfy the following three cumulative criteria:

1. they are **necessary** from a functional point of view to provide effective alternative service provision in the electronic communications sector, taking into account recent technological developments;

2. they are not effectively **contestable** by access seekers given the minimum cost-efficient scale that would be required to replicate the bottleneck and the lack of foreseeable technological developments that would erode the bottleneck qualities identified under criterion (a); and

3. they are **not subject to another viable and functioning access alternative**, irrespective of the legal origins of the access options available; in other words, commercially available access options, obligations imposed under symmetric regulation, remedies imposed under competition law and merger control, and imposed under licence/authorization conditions.

This bottleneck test would be a variation of the existing three criteria test as it combines the entry barriers criterion (no.1) of the SMP test with elements of the competition behind the entry barrier criterion (no.2) of the SMP test. This would seek to reflect the more complex manifestations of market power that are emerging in the digital sector. These criteria would resonate in terms of their relevance across a greater range of areas along the digital value chain. Therefore, the implementation of a bottleneck test would in effect render the spirit of three criteria more important in regulation.

Given the fact that economic regulation aims to protect long term consumer welfare, it would be important that the bottleneck test is administered, and obligations are imposed ***only*** when there is no sustainable competition on the retail markets.

2.3 Complex oligopolies

The liberalisation of the electronic communications sector began with concerns about the implications of monopoly provision. In such situations, full liberalisation meant that an individual SMP-designated operator could be immediately identified in fixed line communications, while individual SMP designations could also be harnessed potentially to address the risk of market power being exercised by an individual mobile operator that generates competitive risks.

The passage of time has demonstrated that fixed line communications have become progressively competitive, with many Member States witnessing incumbent fixed line operators with market shares in retail broadband services that are only marginally dominant according to static market share tests (*e.g.*, >40%, >50%).[15] In the mobile sector, individual operators with those market shares is limited to a very small number of small Member States, with mobile communications markets usually displaying signs of complex oligopoly that are concentrated with 3-4 mobile network operators in each Member State. A small number of joint-SMP cases have been brought in certain Member States under the *EU Regulatory Framework* but have struggled to satisfy that legal standard under the traditional jurisprudence of the European Courts (*esp*. the legal test set forth in *Airtours*),[16] or even the lighter regulatory standard for collective-SMP endorsed in the 2018 revised *SMP Guidelines*.

The challenges faced by policy makers in dealing with complex oligopolies that might generate market failures is something the European Commission sought to address in 2020 when it proposed to introduce a ***New Competition Tool*** which would allow the Commission to commence an extended form of Sectoral Inquiry comparable to the UK's Market Investigation powers. That proposed hybrid legal instrument was supposed to apply in principle across all industrial sectors exhibiting market failure in the context of highly concentrated markets (*i.e.*, in the absence of proof that there existed an individual or collective dominant position) but was focused primarily on addressing competition concerns regarding digital platforms.

Ultimately, the proposal for a *New Competition Tool* was abandoned at EU level (although variants of it are actively being considered in a number of Member States),[17] with the Commission reverting to the express regulation of digital platforms under the *DMA* under a legal standard ("digital gatekeeper") that departs from the competition law threshold of "dominance". Had the Commission pursued the adoption of this new legal instrument, it would have arguably avoided the evidentiary challenges raised by the need to establish a finding of 'collective dominance' and would have focused

[15] The situation might be different in the event that mobile communications markets, which are treated as "cluster" markets consisting of various service elements including retail voice, data, SMS and roaming services, could be fragmented into their constituent elements. In such circumstances, however, competition rules should be well positioned to address anti-competitive behaviour.

[16] Case T-342/99 *Airtours plc v. Commission,* Judgment of 6 June 2002, ECLI:EU:t;2002:146. The collectively dominant undertakings need to have a tacit understanding of how they are behaving in their common interest, they need a sufficient level of transparency between themselves to monitor their compliance with the tacitly agreed common goals, and they have incentives not to deviate from the tacitly agreed goals of collusion (*i.e.*, the existence of some form of 'punishment' mechanism). The test has been applied unsuccessfully most recently in the Netherlands.

[17] The most recent of these initiatives can be seen in the Netherlands. Refer to the respective blogs of Martin Snoep, President of the ACM (29.08.2023) and Paul de Bijl, Chief Economist of the ACM (25.05.2023).

more on the identification of structural concerns which were likely to lead to market failures or which were prone to the exercise of anti-competitive behaviour.

In the alternative, to the extent that the definition of a **'bottleneck'** (see above) **is defined to incorporate channels to customers (as opposed to merely access to physical infrastructure**), a specific instrument designed to address collective dominance through the use of a looser legal standard might not be necessary in the electronic communications context, especially since there is little evidence in the market that concentrated electronic communications markets have produced unsatisfactory market outcomes. A classic example of a bottleneck in these circumstances can be evidenced in the regulation of voice call termination services, ostensibly under the SMP market analysis approach, but more realistically reflecting a bottleneck that is controlled by a number or operators (*i.e.*, restriction of access to an individual customer's number on each individual network) and which the forces of competition cannot overcome or circumvent.[18]

Possible Options

Option 1: ***Reform the existing SMP*** *regime through the replacement of Commission-designated recommended markets (as occurs currently under the Relevant Markets Recommendation) with individual markets that are submitted de novo by NRAs to the European Commission as satisfying the "three criteria test" in national circumstances. This would be tantamount to a residual power of regulatory intervention in the case of situations which necessitate immediate action (and could also involve the greater use of injunctive relief). In turn, the "three criteria test" could be modified to take into account changes in market incentives brought about by technological developments. As an alternative, it could be left up to NRAs to determine which markets justify ex-ante intervention on the basis of the three criteria test, with the possibility being afforded to the Commission to appear as an amicus curiae in national appeal proceedings (which could themselves be subject to an application by the national court for a Preliminary Ruling from the European Court of Justice).*

Option 2: *Replace the SMP test by a* ***bottleneck test*** *which is a variation of the current three criteria test. When retail markets are not effectively competitive, a bottleneck designation may be performed on the basis of three criteria: (i) necessary from a functional point of view to provide effective alternative service provision in the electronic communications sector, taking into account recent technological developments; (ii) not effectively contestable by access seekers given the minimum cost-efficient scale that would be required to replicate the bottleneck and the lack of foreseeable technological developments that would erode the bottleneck qualities identified under the first criterion; and (iii) not subject to another viable and functioning access alternative, irrespective of the legal origins of the access options available. Pursuit of such a policy should take into account a review of real access options currently available to consumers, not merely on the basis of geographic coverage.*

As an alternative, a bottleneck test could be accompanied by a range of ***proportionate symmetric remedies****. The introduction of such an approach would be premised on the understanding that: (i)*

[18] Note, however, that over time, technological developments through the advent of multi-SIM cards and the proliferation of multiple mobile handsets per individual end-user (penetration rates in most Western countries far exceed 100%), have taken much of the anti-competitive sting away from the originally identified market failure.

consumer welfare is unlikely to be impaired significantly by such a change; and, (ii) future investment is likely to continue (or to increase) from current levels.

Compliance costs borne by institutions and regulated firms managing the transition to a new regulatory regime that introduces a new legal threshold should be counterbalanced by clear legislative definitions used to identify bottleneck operators and mandatory remedies being imposed where a bottleneck provider has been designated.

Option 3*: Consider the adaptation of a hybridised legal instrument that is comparable in effect to the* ***New Competition Tool****, with investigative powers being triggered in individually identified cases where highly concentrated markets have yielded market failures or evidenced abusive behaviour. In this regard, consideration should be given to ensuring that sufficient procedural safeguards are afforded to defendants, at least at the level now in place under the DMA. Insofar as ex-ante and ex-poste approaches are offering increasingly more hybridised legal options for intervention, such an approach would arguably address an enforcement gap which currently exists in relation to complex oligopolies.*

An incidental issue which might affect Options outlined above is the need ***to re-assess whether the scope of concepts such as "electronic communications network" and "electronic communications services" need to be expanded or replaced by a broader notion that encompasses more of the value chain that has expanded over time****. In this respect, a more integrated approach could be considered which brings together a wider range of digital communications services. Exploring the scope of such a definitional extension of regulation is, however, beyond the scope of this Report. Caution, however, needs to be exercised not to inadvertently expand regulation so that it catches services best left unregulated altogether.*

3. Regulatory Scope

3.1 Cloud

This Section analyses whether the operators of public Cloud services should be regulated and, if so, under which circumstances.[19] The process of Cloudification and the growing importance of the Cloud as an integral part of connectivity services, including IOT services, has raised concerns among providers of connectivity services that Cloud providers should be considered as legitimate candidates for economic regulation additional to that which they are already subject.[20]

The Commission's *White Paper* asks whether to broaden the scope of the regulatory framework to capture all providers of communications services, regardless of the particular infrastructure used to deliver those services. A widening of the scope of those parties currently captured by today's *EECC* may be necessary, given the changes to the broader digital ecosystem which are taking place. Having said that, this does not mean that they will be subject to economic regulation unless they satisfy the relevant regulatory thresholds for asymmetric regulation.

The proportionality of any decision to extend asymmetric regulation to public Cloud providers, especially given the fact that they are delivering services to all sectors of the European economy rather than supplying only connectivity providers, should take into account the fact that they are already subject to (horizontal) regulation across sectors and across a number of key layers of the digital value chain, including regulation:

- in principle, in their capacity as 'digital gatekeepers' under the *DMA;*
- under a specific Chapter of the *Data Act* in order to ensure that customers are free to switch their Cloud provider;[21] and

[19] Two useful definitions which encapsulate the regulatory significance of the Cloud are found in: (i) the UK Information Commissioner's Office, which states that "*cloud services are digital services that enable access to a scaleable and elastic pool of shareable computing resources*"; and (ii) the US National Institute of Technology, which has declared that "*cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*." The users of public Cloud services are generally firms, with few direct sales to individual customers. Private Cloud services are tailored to the specific needs and preferences of individual customers. Public Cloud services are operated by third party managed platforms, usually involving less sensitive applications and for data storage that does not require frequent access. Hybrid Cloud models are also in use. Most large firms adopt a multi-Cloud strategy.

[20] For example, Cloud services usually satisfy certification procedures in which they must satisfy specific security and compliance standards, especially in terms of security. The Cloud Security Alliance, for example, promotes the use of best practices for providing security assurance within Cloud Computing. These standards are commonly adopted by large Cloud providers. See https://cloudsecurityalliance.org/.

[21] The key competition law investigation issue affecting the Cloud that is common across all jurisdictions (including the ACM investigation in the Netherlands in 2022, France's Competition Authority in 2023, Japan's FTC in 2022, the FTC's investigation in the US in 2022, and the UK's investigation by OFCOM in 2023) is the question of whether customer switching is feasible under current market circumstances. It is this overarching theme which is captured in the specific provisions of the *Data Act*. Among other issues investigated by these Competition Authorities were questions regarding: high egress fees which discouraged switching and reinforced any lock-in effects (which is in theory addressed by the *Data Act*); fidelity rebates in the form of discounts for committed spend which foreclosed smaller Cloud providers with less scale and a more limited range of Cloud-related services (usually considered to be a classic Article 102 TFEU offence rather than a regulatory issue); technical restrictions on interoperability (now also addressed by the *Data Act*).

- In their capacity as digital service providers under the *Network Information Security* (*NIS2*) *Directive*.

Those laws will come into effect over the course of 2024-2025, well ahead of the anticipated timeframe for the review of the current EU Regulatory Framework. However, the likely effectiveness of those measures will only be known once those measures are operational. We are also aware of the fact that, at the time of writing, a series of collaborative relationships between Cloud providers and telecommunications operators have been and are being concluded, which to most policy makers is consistent with a view that the market itself might be able to provide commercial solutions absent regulation (or solutions adopted in the shadow of these other elements of regulation identified above). Moreover, it is also the case that connectivity providers invariably host all of their critical and sensitive data in their own private Clouds, rather than relying on the public Cloud.

Despite the applicability of the various horizontal regulatory measures outlined above, it cannot be excluded that there might be circumstances that could develop in the future that could justify sectoral regulatory intervention on Cloud providers (as suppliers to connectivity providers) that would apply in addition to the existing horizontal regulatory instruments. If, for example, the owners of Cloud infrastructure were at some point to assume the role of "bottleneck" suppliers to connectivity providers, we could foresee a need to incorporate them into sectoral digital networks regulation. If it is appropriate at some point in the future to extend sectoral regulation to the Cloud, however, due consideration needs to be given to ensuring that such *ex-ante* regulation is proportionate, given the existing horizontal regulation to which Cloud providers are already subject.

In a recent report, BEREC has emphasised that the boundaries are being blurred between traditional electronic communications networks services and an evolving range of services made possible because of Cloudification.[22] Indeed, electronic communications networks are evolving both to adapt to the provision of Cloud services and by integrating some of their parts and functions into the Cloud. Connectivity is required for the successful operation of Cloud computing, while the process of network virtualization leads to the use of Cloud solutions and to an increased interest in software capabilities. The blurring of boundaries that is occurring because of these trends is likely to be exacerbated by the advent of new Edge computing services.[23]

While identifying that there may be risks of leveraging by Cloud providers into adjacent telecommunications markets, BEREC also issues the appropriate warning that: "*migration is still at an early stage, technical solutions and standardization are still being developed and experiences may significantly differ*." Accordingly, the overall message from BEREC is that NRAs should closely monitor the evolution of the Cloud, the types of dependencies and relationships that connectivity providers

[22] Refer to BEREC Report on "*Cloud and Edge Computing Services*", BoR (24) 52 of 7 March 2024. It notes at p.8 that: "*Cloud and electronic communications networks and services providers are increasingly intertwined in a double direction client/supplier relationship*".

[23] Note also Commissioner Breton's announcement of a proposal for a future *Digital Networks Act*, where he advocated the creation of: "*the conditions for the sector to fully embrace the technology shift towards cloud-based software-defined models. Telecoms networks are becoming 'network as a service', where connectivity and computing capacity converge thanks to edge technologies and physical switches become application programming interfaces (APIs).*" Refer to https://www.linkedin.com/pulse/digital-networks-act-redefine-dna-eu-telecoms-thierry-breton. In turn, the Commission's associated *White Paper* makes the case for "*technology convergence between telecoms and cloud, which are nonetheless subject to different regulatory frameworks*". This leads to another issue, namely, whether a range of Cloud-related services will, over time, be treated as falling within a broader category of electronic communications service captured by the *EECC* (refer to earlier discussion on regulatory thresholds).

might develop with Cloud providers, and the types of inputs that are provided on an equal footing.[24] Inevitably, the impact of AI on those identified issues might prove to be a critical part of the regulatory puzzle in the future. The "*monitor and see*" message of BEREC is repeated by the Toulouse School of Economics message in March 2024, when it concludes that: "*For regulators, our main message is to exercise some caution*".[25]

If the operators of Cloud infrastructure were to decide to integrate forward to become traditional electronic communications services providers (*e.g.*, providing Internet access services and number-based interpersonal communications services), they could in principle fall directly within the scope of the *EECC.* In such circumstances, the theories of harm that one usually associates with vertically integrated entities with market power could come into play (*i.e.*, high wholesale input prices, the risk of discrimination in the form of self-preferencing, and privileged access to customers). This rationale for such regulation, however, needs to be further assessed in view of the implementation of both the *Data Act* and the *DMA*. As things stand today, Cloud providers do not seem to fit many of the criteria usually associated with "digital gatekeepers" under the *DMA* – especially their absence in playing any dis-intermediation role. By the same token, the *Data Act* purports to address a key aspect of Cloud competition – the ability of customers to readily switch between Cloud providers.

The combination of *DMA* and *eIDAS2*[26] in principle de-couples electronic identification services from the designated platforms (gatekeepers). This opens up mobile phone identification, as provided currently by telecommunications operators, but does not foreclose competition by gatekeepers. This also does not pre-empt the risk of dominant end-to-end control of customers in Cloudified electronic communications. These impacts should be taken into consideration, learning from the experience under the *DMA*, for any future public policy initiatives under electronic communications public policy that could affect the public Cloud.

Possible Options

Option 1: Open up the ***possibility of public Cloud operators being regulated under the SMP standard*** *currently used in the EECC, based on: (i) the identification of a relevant "market" for a wholesale input, contained in a future iteration of the Relevant Markets Recommendation, if and when appropriate (i.e., where the three criteria test can be satisfied); and (ii) subject to definitional changes regarding which parties fall within the scope of the existing EU Regulatory Framework (i.e., currently defined as electronic communications "networks" and "services"). Insofar as Cloud providers supply electronic communications services that satisfy the current definitional criteria, the*

[24] See BEREC Report, at p. 53.

[25] Refer to G. Biglaiser, J. Cremer & A. Mantovani, "*The Economics of the Cloud*", Toulouse School of Economics Working Paper No.1520, 29 March 2024, chapter 5, esp. at p. 42. The Toulouse Paper cites a Cap Gemini Report that also predicts that 5G, Cloud computing and telecommunications will merge to create an interconnected environment that will generate and process colossal amounts of data. The authors cite data which suggest that the market share of the largest three hyperscalers rose from 50% in 2017 to 66% in 2023. Despite this level of concentration, they note that there are potentially numerous competitors that could enter the market and exert competitive pressure on the leading providers of Cloud services. Note the Statement of 8 November 2023 issued in the Digital Competition Communique of the G7 Competition Authorities and Policymakers' Summit, where it was concluded that: "*Significant computational resources such as cloud computing services and large scale computing power also are critical. An inability to access the key inputs may inhibit competition to develop AI and AI applications, reducing innovation and harming consumers.*"

[26] Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93, OJ [2014] L 257/73, as amended by Regulation 2024/1183.

applicability of the EECC is a more straightforward proposition. The application of either the individual or the collective SMP standard is, however, unlikely, because of the current structure of the market (and in the foreseeable future).

Option 2: Open up the possibility of the ***Cloud being regulated under a new connectivity regime relying on the "bottleneck" threshold if and when operators of public Cloud infrastructure services integrate forward into the space currently occupied by connectivity providers****. Although the identification of a bottleneck in the public Cloud space is arguably elusive at this stage of the Cloud's influence on connectivity providers, it would at least not be prone to the limitations of the individual or "joint-SMP" mechanism.*

Option 3: Recourse to an instrument such as the ***New Competition Tool*** *could in principle be used to address market failures identified in a complex oligopoly situation, which at this moment in time arguably characterises the public Cloud sector. By the same token, given the breadth of customers served by Cloud operators, the application of such an instrument only to commercial relations with one sector – electronic communications – would appear to be inconsistent with the manner in which a market investigation tool should operate.*

Option 4: Maintain the current regulatory treatment of ***Cloud providers falling outside*** *the scope of the EECC, based on the understanding that the current SMP standard for intervention would be unlikely to address any future concerns that emerge in relation to providers of public Cloud services, while also acknowledging that the current regulatory interventions due to come into effect at different levels of the value chain in which Cloud providers operate is sufficient to address identified or emerging competitive concerns. The maintenance of the SMP standard would nevertheless remain open to be used in relation to Cloud providers at some point in the future where competitive concerns arise due to their forward vertical integration. As noted earlier, however, such an option might require the extension of the existing definitions of "electronic communications networks" or "electronic communications services" so that they embrace a wider group of market actors than is currently the case.*

Option 5: ***Limit the ex-ante regulation of public Cloud services to something analogous to the DORA regime[27] applicable to the financial services sector****, by treating Cloud operators as "essential providers" to connectivity services. This option suffers from two identifiable drawbacks, insofar as: (i) there is a greater likelihood that it will result in overlapping legislation with the existing legal instruments that regulate certain aspects of the Cloud (e.g., DMA, DSA, the Data Act); and (ii) it would be an approach that is more driven by security concerns than by any perceived need for economic regulation. One can envisage, however, a comparable legislative momentum to DORA may develop in this regard in the Cloud space to provide analogous resilience obligations to financial services, especially given its potential growth with respect to both public and private demand.[28]*

[27] Regulation (EU) 2022/2554, the *Digital Operational Resilience Act* (*DORA*), OJ L 333 of 27 December 2022, pp.1-79. The legislation came into force on 16 January 2023, with the first list of technical standards being published on 17 January 2024. For a discussion on security issues more generally from a regulatory policy viewpoint, refer to the discussion in the *Telecoms Resilience & Security Report*.

[28] As noted above, self-imposed standardization efforts are already being taken up by members of the Cloud Industry Alliance. In addition, large Member States such as Germany and France have already introduced certifications schemes for Cloud providers.

Should that occur, it seems appropriate that the current regulation of the Cloud should be re-considered so that the regulatory response is proportionate and consistent.

3.2 Premium content

The phenomenon of technological convergence means that crucial content acquisition by electronic communications operators has very similar "wholesale input" characteristics to telecommunications services and is of high value in terms of its attractiveness for users seeking broadband connectivity. Perceived shortcomings in the availability of a sufficiently attractive body of content appears to be undermining the greater consumer demand for VHCNs (Very High Capacity Networks). Moreover, there is evidence that, in a number of jurisdictions, access to certain types of premium content, which is a major driver of broadband connectivity, is expensive. Accordingly, questions need to be asked as to whether access to premium content should fall within the remit of EU regulation affecting connectivity.

Traditionally, the demarcation points between economic regulation more generally and the more specific aspects of regulation of content-related services, has tended to identify content-related access jurisdiction as falling within the exclusive remit of the Member States. However, over time, there has been **a growing realisation that the EU has an increasing role to play where content-related issues** veer away from cultural or pluralistic concerns towards market concerns, especially where the latter has the potential to generate negative effects on the internal market. Thus, developments over the past five years have eroded that traditional point of demarcation, and more generally the exclusive power of Member States in relation to various actions taking place in the digital space, as reflected in:

- interventions of the European Commission under EU competition rules and merger control cases (*e.g.*, *Vivendi*) recognising the importance of premium content, the effect of which is to compromise the attempts of large media conglomerates from compartmentalising the EU into exclusive Member State licensing territories;
- the exercise of regulatory powers under the *DSA* as regards the deletion, flagging and removal of illegal content; and
- the prohibition under Regulation (EU) 2018/1807 on the flow of non-personal data of data localisation practices where they distort a single market for data storage and processing services.

Accordingly, taking the above policy shifts into account, perhaps the time is now appropriate for the European Commission to consider whether powers should be conferred upon the appropriate agencies responsible for the implementation of the EU Regulatory Framework so that their powers **extend traditional access regulation to include premium content**. Inspiration for how such a regime can work in practice can be drawn from the UK, which has had such a regime in place for decades, under the supervision of OFCOM. It must be borne in mind, however, that the UK's access to content regime under the *Communications Act 2003* took place under a relatively unique scenario, namely, the interdependence of two platforms over which media content could be delivered beyond digital terrestrial broadcasters (*i.e.*, Sky and the cable TV channels).

The inclusion of premium content access as part of the regulatory access regime would be a policy choice that would arguably be **enhanced by an appropriate governance structure** which empowers an agency with both regulatory and competition law powers, given the complex trade-offs that need to be made under a competition law analysis. In the alternative, workable consultation protocols between competition agencies and regulatory authorities should exist that ensure that both *ex-ante* and *ex-poste* regimes work in unison with one another. In addition, it may be more problematic to have such a premium content access regime administered at national level solely by NRAs, as it is an issue that is prone to a high level of risk of a non-harmonised approach being adopted in light of the different traditions of national content regulation across the EU.

Possible Options

Option 1: *Include access to **premium content as an integral aspect of the access regime under the EU Regulatory Framework**, while having such a regime administered by the **NRAs**, as is currently the case with the access regime in place under the prevailing EU Regulatory Framework (the EECC). The definition of markets for premium content would, however, be likely to be controversial, given the many fragmentations that exist for content in competition law actions and the many variations that are likely to arise as between Member States.*

Option 2*: Maintain the regulatory **status quo** under the SMP regime and exclude premium content regulation from the scope of the access regime applied in connectivity relationship in the EU.*

Option 3*: Have access to **premium content classified as an ancillary or secondary remedy** to the primary remedy used in a market review where it arises. However, this appears to be a unique area of intervention where the European Commission should enjoy a full veto power (similar to its role when vetting market definition and SMP decisions), rather than less binding powers of recommendation.*

Option 4*: Given the policy trade-offs that need to be made in relation to premium content, the advent of ex-ante regulation should only occur where the balance of probabilities suggests that access to the content is a critical element of functioning on the market, without unduly affecting the operation of the market. In this regard, **it is arguably the "bottleneck operator" standard that captures the most appropriate point at which a regulatory threshold is crossed.***

4. Stimulating Network Operator Investments

A range of measures can be considered by policy makers whose effect would be to lower costs for connectivity providers, allow them to develop scale and scope in their operations and allow them greater flexibility in service provision, while helping to grow demand.[29]

4.1 Lowering deployment costs

Input from fixed broadband operators suggest that they **encounter a significant set of administrative costs in relation to the range of permits, licences and authorizations** imposed by local authorities in relation to digging and installation rights for towers, masts and other infrastructure hardware. It was widely acknowledged that, although a number of these obstacles were addressed in the provisions of the 2014 *Broadband Cost Reduction Directive*, a number of important improvements were required in order to expedite the effective and timely deployment of VHCNs.

4.1.1. Fixed networks

The improvements agreed in February 2024 on the final text of the ***Gigabit Infrastructure Act*** **fall some way short of addressing all the open issues that challenge network deployment**. This is particularly the case since those reforms were well overdue after ten years of the initial Directive being in operation (even when taking into account that this was arguably the legislative initiative with the longest and most reluctant transposition into national law). In particular, some of the more significant omissions under the *Gigabit Infrastructure Act*, which will in any event come into effect in late 2025, include exceptions to compliance for:

- small municipalities; and
- infrastructure of "*critical national infrastructure*"; while
- not mandating that tacit approval that would be available in the event of local authority inaction; and
- further delaying operators by subjecting them to conciliation procedures in a potentially wide range of situations.

The *Gigabit Infrastructure Act* specifies that all '*new build*' premises in the EU will need to be connected to fibre networks, as opposed to the less onerous "*broadband-ready*" option that had been considered (Article 8). In addition, provision is made for access to the in-wiring of new or renovated buildings, except where other regulatory obligations render such an obligation unnecessary (Article 9). Several Member States have already implemented obligations along these lines in advance of the new legislation coming into force, and future-proofing broadband competition by ensuring that inside wiring to new buildings foresees the possibility of multiple competitors obtaining access to each individual building.[30]

[29] As regards cost savings, refer also to discussion in Section 3.5 below, "EU-wide service through a centralized platform".
[30] Refer to https://data.consilium.europa.eu/doc/document/ST-6265-2024-INIT/en/pdf.

4.1.2. Mobile networks

As regards mobile networks, the key administrative costs borne by Mobile Network Operators (MNOs) relate to the **high costs of acquiring spectrum and the costs of building and maintaining towers and related infrastructure**, especially given the complications of obtaining permits and environmental compliance considerations. To a large degree, many MNOs have outsourced part of their costing concerns by **divesting themselves of their tower operations**, which are now run extensively throughout the EU by private equity buyers that have often become listed companies. They have also sought to lower costs and to expedite roll-out by increasingly **sharing network infrastructure and spectrum assets**.

Historically, the greatest area of concern for MNOs, however, are the **high costs borne by them for the purchase of spectrum**. These costs are large by international standards (at least when one compares European spectrum fee levels to jurisdictions such as the US where indefinitely renewable licences are available).[31] These regularly recurring spectrum fees with each new generation of mobile technology act as a revenue drain on these operators, which could spend these amounts on network investment and service innovation. Moreover, the high cost of spectrum does not correspond to the relatively low rates of return in the EU from such spectrum.[32] The negative impact of these costs is compounded by the fact that rights of use for spectrum are **not as long as those periods found in other jurisdictions** such as the US, and the fact that new spectrum needs to be acquired with each new generation of mobile technology (although 5G is still in its early stages in the EU, preparations for the introduction of 6G are already underway).

The **auction model for spectrum valuation has been prone to two major setbacks**, both of which have had the inevitable effect of raising its market price. The *first* is the tendency for auction regimes to incentivise incumbent spectrum owners to raise their bidding prices – a classic example of a "prisoner's dilemma", as the incumbent MNO cannot realistically disengage from the auction held from time to time given their sunk costs in developing a network over decades.[33] The *second* setback is strategic, arising insofar as the Member States do not synchronise their auction events to occur simultaneously. This had the perverse effect of having certain MNOs bidding in the early 2000s for 3G rights of use in a range of jurisdictions where they were not realistically capable of winning the bid, but did succeed in raising the costs of their mobile network rivals by bidding high at the earlier stages of multi-phase auction regimes and then withdrawing from the auction. By the same token, auction regimes have the benefit of attaching some meaningful valuation to a public asset (spectrum) and are also less likely to lead to regulatory capture than "beauty contest" procedures.

While some Member States have recognised the adverse economic impact on the industry caused by the shortcomings of auction practices and have preferred over time to adopt 'beauty contests' as the basis upon which spectrum is allocated, many still prefer to benefit from the cash injection to the State's coffers that each auction phase brings.

[31] Direct comparisons on spectrum pricing are rendered more difficult because of this lack of alignment between the duration of the rights covered respectively in the US and in EU Member States.
[32] This is driven by the fact that high frequencies mean that small cells need to be deployed, which results in very high costs in return for little incremental revenue. In such circumstances, even wider coverage does not equate to higher revenues.
[33] In this regard, treating spectrum fees as a necessary 'sunk cost' is somewhat misleading, as sunk costs in most industries either take the form of one-off unavoidable costs or costs that only recur after many years of depreciation of the asset, which require upgrading or replacement. In the mobile communications sector, however, the costs for spectrum recur regularly.

MNOs in the EU appear to be at a disadvantage in their planning of future long-term investments when compared to some of their foreign counterparts in advanced western jurisdictions such as the United States**, given that the average duration of those rights in the EU are much shorter** (*i.e.*, 15-20 years). This often means that some long-term investments are delayed, in preference for funds to be transferred to pay for next generation spectrum auctions. Moreover, the need to obtain authorisation renewals creates uncertainty and the risk of discontinuity, which disrupts investment in other assets until the bidding process has been resolved and tenure is certain.

In addition, because rights of use for mobile spectrum in EU Member States are often shorter than their counterparts in other parts of the world, there also appears to be a reluctance on the part of MNOs to engage in the sort of spectrum trading practices encouraged under Article 51 of the *EECC*, at least when compared to their non-EU counterparts. This reluctance again makes sense in terms of the length of investment cycles, with many MNOs being reluctant to trade spectrum in the face of the need to renew their user rights for the next generation of mobile technology.

The licensing paradigm introduced under the EU Regulatory Framework in 2002 under the *Authorisation Directive*,[34] which envisaged regular recourse to new rounds of licensing renewals in the form of open and transparent bids that were often accompanied by spectrum auctions, is arguably now no longer as appropriate as it was at the time of its introduction. Mobile markets are now mature, and the ARPU generated from expensive spectrum is acknowledged to be relatively low compared to non-EU counterparts, thereby rendering large scale customer acquisition from competing MNOs an increasingly challenging task. In an environment where minimum efficient scale is critical, where next generation infrastructure investment is necessary and where there are barriers to market exit (*i.e.*, including through the workings of the EU merger review policy), the treatment of spectrum as a scarce resource which needs to be the subject of intense and regular auction processes becomes increasingly problematic. In such an environment, the high spectrum fees that have been earned thus far have more to do with existing MNOs being involved in a "prisoner's dilemma" scenario rather than one based on the desire to extract the true commercial value of a scarce resource.

The Spanish authorities have recently undertaken an important policy initiative which appears to have taken such considerations into account, by prescribing that spectrum authorisations for MNOs will hereafter be set for twenty year periods, with the possibility being available for another twenty year period to be available in the form of a renewal.[35] **This "20 + 20" policy, while not of indefinite duration as is the case in the United States, provides MNOs with a degree of predictability within which planning for future investments becomes more straightforward and engaging in spectrum trading becomes a much more realistic commercial proposition** deeper into an MNO's tenure. Of course, certain NRAs might consider it appropriate to introduce obligations on MNOs which reflect the additional value that they have received as a result of an extension of the duration of their rights of use in terms of network rollout/geographic coverage. Although already entitled to do so, a number of

[34] Refer to Directive 2002/21/EC on the authorisation of electronic communications networks and services, O.J. L 108 of 24/04/2002, pp.21-32; as reflected in a more simplified version in. the *European Electronic Communications Code* (*EECC*), O.J. L 321 of 17.12.2018, pp.36-214, at Chapter II "General authorisation", Articles 12-19.

[35] Refer to Article 94(2) of the Spanish *Telecommunications Act*, Spanish Official Journal of 29 June 2022, the aim of which is to promote the "*deployment of modern and innovative electronic communications networks and encourage investment in the sector*".

European NRAs have in practice placed a premium on the receipt of high spectrum fees and, as a form of compensation or set-off, have not insisted on the fulfilment of ambitious roll-out targets.

Possible Options

*(1) We cannot realistically propose that the shortcomings of the **Gigabit Infrastructure Act** be overcome by appropriate amendments which extend its utility, given that this legislation has so recently been adopted and awaits implementation over the next 18 months. Two practical recommendations, however, appear to be feasible: (i) the European Commission should issue **Guidelines** in relation to the **appropriate practices** that should be adopted in relation to inside wiring, as this type of guidance is foreseen under the Act; and (ii) Member State NRAs that have responsibility for the administration of the existing Broadband Cost Reduction Directive and its replacement Gigabit Infrastructure Act should make every effort to make the conciliation **procedure as efficient, cost-effective and streamlined** as possible. NRAs should be encouraged to play an active role in such procedures and, from a governance perspective, Member States should confer powers on NRAs to be the agency responsible for the effective enforcement of the Gigabit Infrastructure Act.*

*(2) Consideration should be given to **mobile spectrum rights of use being of longer duration**, as has occurred under the new Spanish approach (20 years + a 20-year option) in order to allow MNOs to invest in network deployment and improvement rather than on user right renewals. There is every likelihood that such a measure will change the sort of incentives that MNOs have to engage in spectrum trading.*

*As a quid pro quo for this extended duration, however, it would not be unreasonable for Member States to require that the **beneficiaries be obliged to make investments in the short term to ensure that coverage and bandwidth obligations are met quickly.***

Losses in future revenue flows to Member States would be compensated by a potentially much healthier mobile sector, which in turn opens up the possibility of administrative charges being based on the profitability of the sector rather than on a windfall revenue unconnected with efficient use and profitability. The increased level of investment that could be made in response to such an initiative has the potential to act as a set-off against any lost State revenues.

4.2 Demand stimulation

Bridging the identifiable gap that exists between broadband deployment and take-up in the EU is something that probably cannot be achieved solely through private investment, but requires significant measures designed to stimulate demand. Existing evidence suggests that State aid measures to boost broadband deployment across the territory of the EU have been both widespread and generous. Despite these measures, however, the take-up of higher speed broadband offerings has been disappointing in many Member States or regions of Member States. In a number of instances, Member State subsidisation schemes have been prolonged or modified in order in subsequent versions so as to allow greater time in which demand could rise.

Experimentation with different **forms of State aid that are designed to lower the cost of consumer take-up** should be explored more extensively, including not only measures that make broadband offerings more affordable at the point of sale but also other non-regulatory measures which increase the attractiveness of broadband offerings over a long period of time. In the case of SMEs, for example, attractive tax rebates for businesses that use broadband services could prove to be more successful in sustaining demand over the longer term. In this regard also, further thought could also be given to the types of broadband-hungry premium content that can be supported by State measures and to the types of access relations that can be promoted to facilitate the greater availability of premium content offerings over broadband delivery platforms.

Possible Options

Option 1*: As part of a coordinated strategy, targeted schemes of **public support should be explored for the generation of attractive content** which benefits from the growth of VHCNs. Existing programmes to sponsor European-origin content could be expanded to promote broadband-hungry applications. To complement such initiatives, regulatory measures regarding access to premium content (see discussion above) can complement such content creation support measures. The concept of "content" should, however, be seen in a more expansive light than merely entertainment-based services, being linked to public sector applications in the health and educational areas, alongside industrial applications. Such uses provide a much more reliable revenue source, with smaller returns over longer periods providing a more stable investment environment for public sector funding, rather than the more speculative forms of entertainment content.*

Option 2*: The **generation of demand on the part of end-users could be promoted through a variety of State aid measures** that might extend to non-telecommunications matters such as fiscal benefits and tax write-offs for small businesses, which are likely to be major beneficiaries of greater broadband connectivity. While these types of measures technically speaking lie outside the scope of the existing Broadband Guidelines that were updated in December 2022, they could be introduced as part of regional State aid programmes or delivered in the context of pro-European content policies. In the alternative, and additional Chapter could be considered for addition to the Broadband Guidelines which facilitates the use of such ancillary measures.*

Option 3*: European policy makers should consider engaging in a **constructive dialogue with Content Delivery Networks regarding their willingness to subsidise subscriptions** to households that are being/about to be passed by FTTH or for 5G connections. This would appear to be a strategy that is as much in the interests of such operators as it is for public policy makers. A dialogue along these lines could form the basis of future cooperative efforts with respect to the development of AI and Virtual Reality, which might arguably form an even stronger basis in the near future for the growth in demand for high-bandwidth applications.*

5. Technology Transition

Irrespective of the particular regulatory threshold that might be preferred for the triggering of *ex-ante* regulation for connectivity providers, consideration needs to be given to whether the types of access obligations which the subjects of regulation might need to satisfy are fit for purpose. To this end, we consider below a number of changes that could be considered in relation to the existing EU Regulatory Framework, as is currently embodied in the *EECC* and in the recent adoption in February 2024 of the *Gigabit Connectivity Recommendation* and the *Gigabit Infrastructure Act*. To the extent that these recently adopted legal instruments have sought to deal with a range of access-related issues in a comprehensive manner, we have not explored further options unless further clarity is deemed to be necessary on the scope of such measures.

5.1 Copper switch-off

Given that the overarching goal of the European Commission is the satisfaction of its Digital Decade objectives, coupled with the climate goals that need to be satisfied by the year 2050, it needs to be asked whether the satisfaction of this goal is compromised by the continued reliance of incumbent fixed line operators in certain Member States in utilising their traditional copper networks. **Some commentators suggest that ADSL is slowing down the deployment of fibre**.[36] The question which needs to be asked is whether the offer of sub-optimal access alternatives has a negative impact on the investment incentives of fixed incumbent operators and on the investment incentives of access seekers as regards the rollout of VHCNs.

As suggested in the Commission's *Digital Networks White Paper* introduced in February 2024, **copper networks could be subject to a mandatory switch-off in the year 2030**; even if there is some slippage in certain Member States regarding this timeline being met, it appears to be inevitable that copper networks in Europe will be switched off within the next decade.

By the same token, access seekers in many Member States are satisfied to receive wholesale access via copper networks at lower wholesale prices than the prices they pay for access to fibre-based networks. In turn, this provides them with a greater profit margin at the retail level where they compete with incumbent fixed line operators in the provision of relatively low-capacity broadband services. The **wholesale pricing flexibility afforded to NRAs under the *Gigabit Connectivity Recommendation* should in principle allow NRAs to 'nudge'[37] alternative operators away from legacy copper networks**.

Seen in this light, if State subsidies are available to encourage technological migration that facilitate the economically attractive transition from copper to VHCNs for incumbent fixed operators, consideration should also be given to *compelling* operators to migrate away from copper-based

[36] Briglauer, W., Cambini, C. and M. Grajek (2018), "*Speeding up the internet: Regulation and investment in the European fiber optic infrastructure*", International Journal of Industrial Organization, vol. 61, showing that a lower access price to copper decreases the fiber investment of incumbent operators; see also Bourreau, M., Grzybowski, L. and M. Hasbi (2019), "*Unbundling the incumbent and deployment of high-speed internet: Evidence from France*", International Journal of Industrial Organization, vol 67, showing that a higher number of competitors through local loop unbundling in a local market implies less deployment and coverage of high-speed broadband.

[37] The expression often used in academic jargon to indicate a policy preference which is driven by changes to commercial incentives of market actors, rather than outright prohibitions or mandatory specifications.

solutions. In this regard, **specifying a digital cut-off date might be seen by some policy makers to be necessary, but only given the appropriate support measures available to ensure a 'soft landing' over a reasonable transition period**. Such a cut-off date would be accompanied by migration measures comparable to those currently available under Article 81 *EECC*. The 2024 *Gigabit Connectivity Recommendation* deals with access pricing for copper-switch-off (at paragraphs 76-81), which appears to provide reasonable policy trade-offs for smaller market actors.

By the same token, given the fact that there is little tangible 'harm' that is being experienced by end consumers who have shown a reluctance to embrace high-capacity broadband services in many Member States, perhaps compelling such a change in investment behaviour is not a proportionate measure. In addition, a mandated change away from copper networks, if prescribed over a short period of time, might leave operators whose business case relies on wholesale access 'stranded' (similar to the manner in which energy producers from non-renewable sources have 'stranded' assets and are compensated by State aids programmes). A counterweight to these arguments, however, can be identified in the benefits that can be derived from a full switch-over to VHCNs from the viewpoint of the *Green Deal* objectives that are being satisfied.

Possible Options

Option 1*: Prescribe a **hard cut-off date for copper switch-off**. Such a path is, however, problematic in a number of respects. For example, one cannot rule out that a policy along these lines would be subject to legal challenge under Article 345 TFEU, which prescribes that:" The Treaties shall in no way prejudice the rules in Member States governing the system property ownership." In addition, a legal challenge might be lodged under the terms of the EU Charter of Fundamental Rights (although Article 17 envisages interference in property rights when justified "in the public interest").*

Moreover, even if such a measure is held to be in compliance with the European Treaties, a proportionate response would be for the Commission to provide a clear migration path for access providers which does not destroy the business model of access seekers in the short run. At the same time, consideration should be given to the modification of the notion of "technology neutrality" (see below) with a view to ensuring that access options will continue in the marketplace as a matter of technological possibility, as opposed to regulatory necessity. To this end, clear migration criteria would need to be established according to the legislation, rather than leaving the degree of flexibility provided in Article 81(2) EECC in the hands of access providers.

In adopting a hard cut-off date approach, it would perhaps be best to adopt a more flexible policy by mandating copper switch-off for a designated [X] number of years where fibre penetration rates in a given region reach a level of [Y]. In that way, clear migration paths can be foreseen in advance and legitimate expectations of market operators can be protected more proportionately.

Option 2*: Where rational economic incentives do not exist for a migration to fibre by an incumbent operator (estimated to be limited in number), **fixed incumbent operators could be subsidised to incentivise their migration from copper to fibre** networks (VHCNs) as quickly as possible. Again, a migration path will need to be carefully constructed which builds upon that already found in the EECC so that existing access seekers do not find themselves economically stranded. To this end, the consideration should be given to the possible amendment of the Broadband State Aid Guidelines so*

that this form of subsidy to an incumbent operator would be compatible with State aids principles. In addition, the subsidisation might incorporate the possibility of more advantageous access prices being made available where access is sought to the State-subsidised VHCN in question.

This arguably provides a balanced solution in terms of satisfying the interests of both access providers and access seekers alike. It would also avoid having stranded assets and would not undermine the preferences of consumers in certain Member States insofar as they remain content with broadband services delivered over copper network connections. Having said that, the incentives for migrating to fibre in most cases are well understood, which means that any subsidisation that takes place should be focused only on those situations where incumbents have no tangible incentives to migrate to fibre. Given these circumstances, reliance on further State subsidies may be a disproportionate option.

Option 3*: Adopt the approach already advocated by the Gigabit Connectivity Recommendation, namely, allow* ***flexibility to network operators for their wholesale copper pricing to rise****, thereby incentivising access seekers to prefer fibre broadband connections because their margins will not be significantly lower if they opt for fibre broadband connections.*

The pursuit of this option achieves a balanced result of migration from copper to fibre and would help fixed incumbent operators to improve their profitability, although it has the potential to adversely impact access seekers insofar as it threatens to lower their margins significantly. This option is also preferable to an approach which mandates an absolute cut-off date, because the latter would provide a very 'hard landing' for access seekers and may not be desirable for certain end-users who do not feel they require more advanced broadband offerings at higher prices; this can arguably be avoided by regulators prescribing that a copper-equivalent service continues to be offered (e.g., as occurs today in a Member State such as France).

Option 4*: Continue with the current* ***status quo****, largely because end-users in many Member States are satisfied with the current level of broadband functionality and because many access seekers are content with the access offerings available today, such as VULA products. Such an approach, however, pre-supposes the continued regulation of access on the basis of the SMP standard.*

5.2 Technological neutrality

The application of the concept of technology neutrality is widely considered to be a cornerstone of the existing EU Regulatory Framework since 2002 (including its latest iteration under the *EECC*). Yet, despite its importance, **the concept of technological neutrality has been used flexibly**, to the extent that it has been referred to in various legal instruments across the digital arena in three particular (but very different) contexts, namely: (i) that regulation should prescribe objectives but should not prescribe the specific technologies that are used to achieve those objectives;[38] (ii) the same regulatory

[38] This involves setting clear targets and characteristics to be favoured by policy makers and then letting the best technologies emerge. While the concept is not necessarily 'agnostic' as regards market outcomes, but it is agnostic as regards the technologies that are used to deliver the specified outcomes.

principles should apply regardless of the technology being used; and (iii) regulatory authorities should refrain from nudging the market towards the use of a particular technology.[39]

In the past, reliance on this concept was the basis on which upgraded copper network solutions were deemed to be equally valid to fully fibre network solutions, even though the latter had many advantages, and the former had clear limitations in terms of its ability to continue to evolve in terms of latency, speed and other parameters. As a result, a number of Member States prioritised upgrading copper to the detriment of full fibre network deployments, especially where the copper option was more economic. While the concept tends to be associated with the actual technology being used (copper, fibre, *etc*.), today it is arguable that it can **also legitimately apply to technology architectures**, where a more nuanced approach is also necessary. If the architecture is such that core public interests such as national security is not safeguarded, for example, a legitimate reason might exist to intervene at an early stage (a case in point being 5G security). Architectural choices that are made early on such as those for modularity, interfaces and interoperability, should be such that future markets remain contestable. While the task of regulators is to ensure that market behaviour is in conformity with these public policy goals, their competence does not extend to the specification of network architectures and technologies, which is a power that needs to be delegated to other bodies.

The concept has also been indirectly associated with the **process of market definition**. This is because the concept of substitutability, which lies at the heart of the market definition process, means that alternative technologies that perform the same task should be considered to fall within the same relevant product or service market. This, in turn, has the effect of potentially broadening the relevant product or service market, as is reflected in the terms of recital 14 of the *EECC*.

Finally, the application of the concept also means that regulators are limited in practice in their **choice of remedy**, as they cannot prescribe certain technology-specific measures, irrespective of their effectiveness in addressing an identified competition problem. This is yet another aspect of the mantra that regulators should not be put into the position of choosing "winners and losers" among providers of different technological solutions, although the Commission has shown its willingness to back away from the full application of the concept in practice in the context of a number State aid funding mechanisms.

Despite the relative importance of the concept as a central tenet of EU policymaking, it should not be forgotten that arguably **Europe's most significant technological development – the adoption of the GSM standard – is an example of departure from the concept of technological neutrality**. In that case, an industrial policy choice was made to select a particular technology. By contrast, the concept has been harnessed by some broadband operators to select technologies that ensure that their networks are effectively 'closed' to competitors at the retail level, despite delivering high quality broadband services to their retail customers.

The concern is that **strict adherence to the concept might not lead to the optimum results** that could be achieved either with respect to effective access solutions or with respect to the deployment of technologies that fulfil the goals of the *Green Deal Agenda*. To some degree, this has already been acknowledged in the text of the *EECC*, which provides for some narrow exceptions to the application

[39] Refer to discussion in W. Maxwell & M. Bourreau, "*Technology Neutrality in Internet, Telecommunications and Data Protection Regulation"*, Computer & Telecommunications Law Review (2014).

of the technology neutrality concept where the circumstances justify such a departure. If, however, a de-regulatory path would be followed, **the prescription of technologies that can facilitate access and can satisfy foreseeable broadband capacity demands** would be a highly desirable outcome; this is especially the case where access seekers are migrating from an access model based on regulatory prescription to one based primarily on commercial negotiation. It could also accommodate multiple broadband providers gaining access to newly built premises, especially given the requirement in the *Gigabit Connectivity Act* that all new-builds must be able to accommodate fibre networks.

Accordingly, in the event that the SMP standard were not to survive the re-assessment of the regulatory framework, the *quid pro quo* for adopting such a decision could be to adopt **open technological standards** that would apply to newly deployed networks so that open access would in principle be available without any of the technological challenges that restricted access to cable TV networks for so many years. In addition, such an approach would arguably be in furtherance of the EU's *Green Agenda* goals.

Moreover, the policy proposed by the European Commission in its *Gigabit Connectivity Recommendation*, by **incentivising parties to migrate to broadband networks at the expense of copper networks**, has arguably already carved out a very large exception to the concept of technology neutrality. Such a policy would arguably establish a technological pathway that would be robust for the upcoming decades.

Possible Options

Option 1*: **Retain the concept of technology neutrality but clarify that the concept is bound to outcomes** in the pursuit of broader policy objectives. Adherence to the concept has been an integral part of a process of market definition and SMP designation, and acts as a mechanism by which the proportionality of remedies can be measured. Insofar as the SMP standard is retained, the rationale for departing from a clarified technology neutrality concept is less compelling and should be limited to specific situations which are compatible with the satisfaction of Green Deal targets and the goal of an interconnected connectivity ecosystem.*

Option 2*: **Remove the concept of technology neutrality** altogether as a policy driver from the EU Regulatory Framework insofar as the SMP-standard for regulation is no longer pursued. Future-proofing access relationships requires that positive policy choices about technology be made so that all parties have a transparent basis upon which to base interoperability and cooperation in a value chain which has the hallmarks of a complex ecosystem.*

Option 3*: Further **modify the scope of the concept of technology neutrality** by defining those areas where the relevant NRA has the power to specify a range of open access technological solutions which are based on clear policy priorities and which are susceptible to appropriate standardisation procedures that cannot be 'gamed' by industry. On balance, if it is decided by policy makers to depart form the existing SMP regulatory standard, it appears to be justified to have a clearly **articulated approach on the limits of technological neutrality. Such a policy would explain the policy objectives that should be achievable** where parties wish to rely on the use of a particular technology.*

6. Competition Law

There may be a tension between, on the one hand, regulatory incentives for European connectivity providers to achieve greater scale and scope capabilities through collaborative efforts or through acquisition and, on the other, traditional competition policy which may take a dim view of such actions undertaken by parties with market power (irrespective of the industrial sector involved). These impediments to growth are considered by the many connectivity providers as essential to their continued viability at a time when their commitment to investment is required to complete the internal market for digital services. The issue is therefore whether legitimate shifts or trade-offs in competition policy principles can facilitate or hinder this process, without jeopardising the fundamental elements of competition policy.

The European Commission's recently revised *Market Definition Notice*[40] provides the opportunity for at least some of these trade-offs to occur consistent with the Commission's own policy orientation. For example, the Notice explicitly acknowledges the **European Commission's willingness to conduct dynamic and forward-looking assessments**, especially in markets undergoing structural changes, especially where they are of a technical or regulatory nature.

There are a number of **technological developments currently affecting the connectivity sector** (Open-RAN, slicing, de-layering, along with Wholesale-Only provisioning over fixed networks, *etc*.) that should be taken into account in a forward-looking competition analysis. Open-RAN may imply that there are less technological path dependencies (and therefore less gains from multiple paths chosen), while network slicing could imply something akin to a WDM overlay on a fixed network topology. This could establish the conditions for differentiated network services to be provided and, indeed, technological independence in a mobile context also. At least the impact of these technologies may render commercial partners more independent of one another, which may in turn mitigate the risks of collusion concerns in some cases.

The possible weakening of market power as a result of the technological changes identified above also needs to be considered in the broader context of the general economic state of the telecommunications sector in Europe, which is having an impact on the structure of the sector. For example, the Return on Capital Employed (ROCE) is a calculation that reflects the degree of competition in the market, insofar as more competitive markets will see ROCE figures closer to the Weighted Average Cost of Capital (WACC). This is not normally problematic, as long as ROCE covers WACC (which generally appears to be happening). Concerns may exist, however, in those situations where the ROCE figure is very close to the WACC figure and either WACC rises quickly or there is a period of intense competition to build market share. These scenarios will be problematic if there are more operators than **minimum efficient scale implies**, and/or where there is a very restrictive consolidation (merger) regime in place. In this case, the concern might arise that investment would not be sustainable in the longer term.

The low ROCE figures need to be further considered in light of the observation that competition has generally worked well in traditional telecommunications markets. These markets are delivering good services at low prices in situations where ROCE is generally close to, but covering, WACC. Importantly,

[40] Document C/2023/6789, OJ C/2024/1645 of 22.2.2024.

investment is growing in most markets. However, if connectivity providers (and the stock market which measures their financial viability) perceive that this situation will not persist and that ultimately ROCE will fall below WACC,[41] while at the same time market stabilisers such as exit (via consolidation)[42] are not available, it is more than possible that their **willingness to invest will be impaired in the longer term**. To ensure that long term willingness to invest is preserved, a review of the various mechanism to correct those situations where ROCE is below WACC may be needed.

6.1 Article 101-102 TFEU

At a most fundamental level, the **encouragement of co-investment relationships under the *EECC*[43] has not resulted in a level of investment that was anticipated** at the time the *EECC* was enacted in 2020. This may be partly due to the complexity of the co-investment provision in the *EECC*, but also to the fact that co-investment relationships involving fixed incumbent network operators, despite being supported by the *EECC* and by the guidance provided by BEREC, also trigger competition law review procedures either under Article 101-102 TFEU or under merger control rules (depending on the level of integration between the participating parties to the co-investment). This has meant that such arrangements have not only experienced delays before their final clearance by two legal regimes acting in parallel, but also because a competition law analysis is likely to be more onerous than a regulatory review under the *EECC*.[44]

Accordingly, if one specialist legal regime is designed to foster investment while, on the other hand, a general legal discipline is designed to promote competition, there may be tensions in enforcement strategy and delays in implementation. This means that **coordination is desirable between the approach undertaken by NRAs when reviewing co-investment decisions under the EECC and NCAs/European Commission when reviewing those same arrangements under Article 101 TFEU or the *EU Merger Regulation***. This is necessary to avoid an unnecessary duplication of administrative effort, the generation of avoidable costs and delays, and the risk of conflicting enforcement messages. Ultimately, it is important for investment certainty in the sector that the respective *ex-poste* and *ex-ante* regimes are aligned in their approach to network sharing practices.

In addition, tensions may also arise in relation to the endorsement offered under the *EECC* to infrastructure and spectrum sharing relationships[45] in the face of the traditional approach taken by

[41] As might be anticipated with flat EBIT and rising Capital Expenditures in the move to 5G SA.

[42] The existence of exit barriers in mature electronic communications may mean that smaller operators are not able to realise the value of their investments, while at the same time not being able to invest in innovative technologies because the acquisition costs for each new subscriber exceed their projected ARPUs.

[43] *EECC*, Article 76.

[44] The evidence of how a co-investment scheme in Italy over two years ago has now morphed into a prospective merger in early 2024 involving illustrates the impact of delay and uncertainty in relation to investment incentives. While it would not be unreasonable in other legal systems to argue that the *EECC*'s co-investment regime establishes a *lex specialis* which should in principle override *ex post* concerns that apply across all sectors of the economy, that is not the scenario that exists in the EU, since Article 101 TFEU is primary law which cannot be overridden by sector-specific rules: see N. Dunne, '*The Role of Regulation in EU Competition Assessment*' (2021) 44(3) World Competition 287. Perversely, it would appear that the many years of delay in having both the regulatory and competition law regimes approve a co-investment scheme in Italy that would have had various access obligations attached to it have led to the fixed Italian incumbent ultimately being bought by a private equity group without any such conditions being imposed under an *EU Merger Regulation* analysis (official clearance Decision of the European commission pending – see Reuters, 24 May 2024, "*KKR set for unconditional EU antitrust okay for Telecom Italia deal, sources say*", Foo Yun Chee & Elvira Pollina.

[45] *EECC,* esp. Article 45. Refer also to Commission Communication on "*Promoting the shared use of radio spectrum resources in the EU*", COM/2012/0478 Final; *cf.* BEREC-RSPG Report on "*Infrastructure and spectrum sharing*", BoR (1) 26 – RSPG-374, June 2011.

competition authorities that may be reluctant in some cases to approve cooperative relationships between competitors without the offer of significant concessions.

Competition law enforcement under Articles 101-102 TFEU should take into account **major technological changes, particularly those of softwarization and virtualization, both of which contribute to the dis-intermediation of network and service layers.** As noted above, these changes have driven the focus of activity from the centre of the network to its periphery, thereby potentially changing in some cases the commercial incentives of network providers to engage in anti-competitive behaviour. In addition, the proliferation of RAN technology means that each network can host multiple operators, which can replicate their own 'network' characteristics when dealing with their respective customer bases. Thus, the technological changes may have the potential to erode network operators' market power by virtue of their operation of a physical network in a number of material ways. They also have the capacity to increase the countervailing bargaining power of other digital market actors that wish to be hosted on their networks, which has now been made possible by RAN technology.

As a result of these technological changes, we foresee possibilities that concerns about foreclosure, leveraging and anti-competitive 'spill-over' may become less important over time because critical commercial incentives and the ability to engage in such practices may be muted by technological change; this is largely because the ownership of underlying physical assets delivering services could no longer constitute a significant competitive advantage. **Network virtualization** techniques will lower barriers to entry and could increase competition in numerous markets (including cross-border markets) assuming that appropriate access to these virtualized elements is available ('virtual access').

As BEREC has acknowledged, some of these technological changes mean that networks are becoming increasingly 'hardware agnostic'. The process of network virtualization and the impact of **network dis-intermediation** also create a situation where the traditional distinction between 'active' and 'passive' network sharing becomes less problematic as software on the edge of the network becomes the key determinant of quality differentiation (rather than the control of a network).

The technological realities of 5G network deployment also suggests that the usual 'bright lines' between the analysis of urban and rural network sharing arrangements may need to be re-considered on a case-by-case basis. This is because network deployment costs under previous generations of GSM technology have been much more expensive in rural areas due to the high levels of expenditure needed to provide coverage for areas with low population density in those rural areas. By contrast, the realities of 5G rollout require the deployment of greater numbers of base stations because of the use of certain spectrum bands; by the same token, that increase in capacity decreases the range required for more network infrastructure to be deployed.

As hardware used in 5G becomes increasingly commoditised and the general move to SDN and NFV continues apace, the focal point of competitive activity is likely to move to the software that runs over the hardware and to the services that are delivered over that hardware. **These factors are consistent with a high degree of decisional autonomy on the part of network participants**. This degree of autonomy leaves a pathway open for regulators to take a different approach towards network sharing that otherwise would have been problematic under a competition law analysis delivered under a more traditional technology paradigm (especially as regards the different approaches taken traditionally between 'active' and 'passive' sharing elements).

Aside from the general observations made by the European Commission in its revised *Market Definition Notic*e in early 2024, these observations on changed incentives could also have been reflected more precisely in the Commission's *Horizontal Cooperation Guidelines* that were already updated in 2023.[46] In its Press Release in the recent *Czech Network Sharing Case*, however, which dealt with 3-4G network sharing, the Commission has indicated that its Decision was *without prejudice* to the approach it might be willing to adopt in the context of 5G network sharing arrangements. We consider this important caveat to signal an approach that might embrace the logic of fundamental technological changes identified in our discussion above. More generally, the Commission notes that network sharing in 5G networks should be considered positively because a reduction in the cost of deployment can speed up deployment, increase network coverage and allow for the more efficient use of spectrum, all of which benefit the consumer.[47]

From this perspective, the *Horizontal Cooperation Guidelines* can arguably now be read in light of the European Commission's more recent observations in its revised *Market Definition Notice*, allowing for a greater focus on general principles that frame the assessment. If this is done, the Commission can be seen to be generally favourable towards network sharing, with competition concerns arising when these agreements affect the quality of service and prices at wholesale and retail levels. The **appropriate legal test should therefore not be a static one that focuses solely on the degree of network sharing but one that is more focused on examining, in its specific legal and economic context, the likely effects of network sharing**.[48]

While each form of cooperation will need to be evaluated on its own case-specific merits, operators should nevertheless have at their disposal the analytical tools needed to form a judgement as to whether Open-RAN sharing for 5G deployment in urban areas can be pursued under Article 101 TFEU in light of new technologies, and what measures are appropriate and proportionate to ensure the competitive independence of the parties involved in the sharing. Because VHCN and 5G deployments are linked due to their common use of small backhaul sites, **the reduction of legal uncertainty on Open-RAN sharing in densely populated areas would facilitate investment in both VHCN and 5G technologies**.

Given the tenor of the *EECC* and the Commission's *Recommendation on Connectivity* - which expressly encourages network sharing – the provision of general guidance on how **technological developments in 5G may affect its competition law analysis of Open-RAN sharing under Article 101 TFEU** seems to be an important policy imperative that should be addressed.

In the case of **spectrum sharing**, the Commission's *Horizontal Cooperation Guidelines* reflect the traditional competition law approach about the compatibility of those arrangements with the prohibition on competitive restrictions found in Article 101(1) TFEU. The terms of the *EECC* and the administrative practice of a number of NRAs (but not all) are consistent not only with granting

[46] Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements [2023] OJ C259/1. For example, while the Commission included a separate discussion in its *Guidelines* on mobile network sharing and spectrum sharing (paragraphs 259-266) that reflected its historical concerns regarding these types of relationships between competitors, it could have expressed a view on the impact of recent changes brought about by technology (especially the impact of RAN technology) that could influence its competitive assessment of such agreements.

[47] *Horizontal Cooperation Guidelines*, at footnote 181.

[48] *O2* (*Germany*) *v Commission*, Case T-328/03, has already encapsulated this lesson, whereby a formalistic analysis was quashed in favour of an emphasis on the economic effects of the agreement.

permission for, but also facilitating, various aspects of spectrum trading and sharing. From a technological point of view, it is also arguable that spectrum sharing does not pose the same concerns as it may have done in the past because the move to Open-RAN means that a high degree of technological independence can exist over a shared RAN.

6.2 Merger control

The designs of mobile operators to achieve in-country scale have on a number of occasions fallen foul of the European Commission's strict stance as regards 4-to-3 mergers in the sector in the wake of the exercise of its powers pursuant to amendments made to the *EU Merger Regulation* in 2004. These amendments expanded significantly the Commission's powers of review into so-called "gap" cases (*i.e.*, restrictions of competition identified in market structures somewhere between unilateral effects and coordinated effects).[49] The continued recourse of mobile operators to consolidation attempts, despite the possibility of having their merger blocked or subject to sweeping commitments designed to introduce viable new competitive entrants post-merger, pays testimony to the importance of market exit possibilities in the mobile sector. **These powers in relation to gap cases were clarified in 2023 in the *CK Telecoms Case*** before the European Court of Justice.[50] In brief, the Court of Justice ratified a multi-factor approach in testing whether a merger may substantially impede effective competition.

Given the general evolution of competition law towards a more dynamic approach, time may be appropriate for the **Commission to consider adopting a more dynamic view in relation to the consumer welfare and harm that might arise from these consolidations in the mobile sector, especially by taking a broader view of consumer welfare interests in the mobile sector beyond short-term negative price impacts**. To this end, such an approach could accord due weight *inter alia* to such factors as the following:

1. Changes to economic incentives brought about by **technology** (see above) might mean that it is not necessary to have more than three Mobile Network Operators (MNOs) in order to sustain a heathy access regime.

2. The fact that **bundled offerings** can be provided over different platforms means that the identification of market power in individual MNOs might be illusory, especially where the different platforms are able to source all the necessary inputs of the bundle available to mobile operators and incremental price rises in one sub-set of the bundled offering can be offset by super-competitive offerings from other sub-sets of the bundled offering.

[49] Refer to the discussion of these cases in the Annex to this Issue Paper.
[50] Case C-376/20 P, *Commission v. CK Telecoms Investments Ltd*, EU:C:2023:561.

3. The participation of MNOs in a **broader digital ecosystem** not only means that they are challenged by actual and partial substitutes, but that there are different sources of market power and countervailing bargaining power that might restrict their ability to exercise or leverage market power. The consistent pattern of collaboration between digital platforms and MNOs confirms the increasing commercial interdependence of the latter and the former.[51] The application of an approach which focuses on the analysis of "ecosystems" as the basis for intervention in digital platforms can and should be used just as readily – where appropriate - to justify why mobile mergers present few competitive risks when mobile services are provided within a much wider ecosystem of digital services.

4. In comparison with the approach taken in relation to mobile sector mergers, the Commission has taken a consistent approach both under merger control and increasingly under *ex-ante* regulation, which considers that competition in the **fixed line sector** may be sufficiently robust if there are at least two effective access options available to access seekers, with the possibility that a third access option might materialise. Although it is true that the mobile cases focus on the impact of the 4-to-3 consolidation on end consumers at the retail level, while the fixed line precedents focus on the state of competition at the wholesale access level, it seems appropriate that further thought be given as to how the approach taken towards competitive assessment across both the fixed and mobile sectors should be harmonised.[52]

5. Independent analysts such as WIK and sector-specific regulators such as OFCOM have suggested that the **scale required to sustain an efficient operator** in a 5G environment means that the optimum average number of MNOs in a national market may be three. Insofar as these views are driven by the particular technological configurations associated with 5G technology and the levels of investment required to deploy 5G and subsequent generation mobile technology, these views need to be considered carefully.[53]

6. Moreover, when considering **efficiencies**, there is a case for according greater weight to the benefits arising in the medium to longer term in terms of more investment, growth in service and resilience in network security. At present, the emphasis is virtually only on the short-term impact on consumers (refer to the discussion in the Annex to this Report).

Possible Options

(1) ***Greater coordination is required between the pursuit of regulatory goals under the EECC and competition law instruments****. Such coordination can be particularly helpful in building a shared awareness across the Commission about the impact that technological changes can bring to the*

[51] For a detailed discussion on various aspects of the mobile ecosystem, refer to the UK's Competition & Markets Authority report: *Mobile Ecosystems Market Review*, dated 10 June 2022.

[52] The wave of consolidation in the sector is proceeding apace, as is reflected in the recent European Commission approval of the merger in Spain involving *Orange/MasMovil* (Case M.10896 of 20 February 2024) and the pending reviews at the time of writing by the respective Italian and UK National Competition Authorities of the *Swisscom/Vodafone Italia* transaction and *CK Hutchinson/Vodafone* UK transaction. Whether or not a more expansive review of consolidation is a likely short term policy option will be shaped by this new wave of consolidation.

[53] For example, refer to https://www.ofcom.org.uk/_data/assets/pdf_file/0036/248769/conclusions-mobile-spectrum-demand-and-markets.pdf (at footnote 80). Refer also to https://www.ofcom.org.uk/_data/assets/pdf_file/0027/231876/mobile-strategy-discussion.pdf (at Box 6.4)].

competition law analysis to be carried out in the future, which can justify a departure from traditional enforcement priorities.

(2) Because ex-ante and ex-poste regimes are arguably pursuing complementary policy goals, it would be more constructive for ***competition rules to adapt their reference points*** *in individual cases as regards how best to assess anti-competitive concerns in relation to connectivity relationships,* ***paying particular attention to the impacts generated by technological changes such as virtualization and softwarization.*** *These change in approach should be reflected both in the Commission's administrative practice under both Articles 101-102 TFEU and under its review of mergers under the EU Merger Regulation. Precedent for the adoption of such an approach can be found in the recent adaptation of energy sector policy under the Energy Market Design Proposal, which creates a unique regime in which regulation has an impact on the way in which competition rules assess the compatibility of long-term energy contracts.*

(3) A greater ***focus on sustainable competition and longer-term benefits*** *in terms of increased investments with a view to providing innovative services, in tandem* ***with a more nuanced application of efficiencies defences****, could yield advantageous results for merger review, without running the risk of sacrificing the benefits already achieved for European consumers. Each individual case should be judged on its merits and the notifying parties should continue to responsible for tendering evidence about the positive implications of their mergers. When* ***remedies are imposed, they should promote sustainable competition*** *and the long-term interest of users.*

7. Strengthening the Internal Market

It is undeniable that one of the over-arching political goals of the EU is the creation of an internal market for digital services, with the provision of mobile connectivity being an essential component of that goal. Mobile communications have always held a special place in the goal to create an internal market, especially given the fact that mobility via roaming by definition fosters cross-border connectivity. That impetus should be amplified with the greater penetration of IoT services, many of which will require trans-border provisioning. The provision of services to trans-national business customers has also been a critical element in the growth of communications markets at a European level, combining components of both fixed and mobile service offerings built largely upon assets that are leased from local operators.

Aside from a potential overhaul of spectrum pricing (see discussion above) leading to cheaper operating costs for MNOs desiring to have a pan-European footprint, a number of other policy initiatives need to be considered in order that mobile networks are able to fulfil their potential to create an internal market.

7.1 EU-wide services through a centralised approach

Unlike operators in many other jurisdictions, **European connectivity providers bear costs because they are not in a position to provide EU-wide services without satisfying national regulatory requirements in all 27 Member States across a wide range of matters**. This is despite the fact that a series of developments in technology (particularly the availability of virtualized networks) have made it easier for connectivity providers to physically provide services over a much wider geographic area than ever before. The costs of compliance are especially high in those situations where connectivity providers supply services to a relatively small number of business customers across a wide range of EU Member States. For example, national rules imposing obligations regarding **network security, lawful interception, data retention or localisation of Security Operations Centres can act as a barrier to the establishment of a Single Market**. In addition, the proliferation of local documentation requirements to complete relatively *pro forma* authorizations and to satisfy local administrative obligations multiply unnecessary costs which do little to promote important national strategic goals while adding unnecessary costs to service providers; these costs borne by service providers are ultimately passed on to their business customers.

There **do not appear to be any insurmountable obstacles to putting measures in place that would allow the delivery of administrative obligations, including lawful interception and other security measures, to be hosted centrally and delivered in multiple European territories.** While providing those services to individual end-users might raise greater concerns about security and consumer protection compliance, those concerns are negligible in the case of contracts negotiated with sophisticated industrial users, especially where many of these contracts are centrally negotiated at the corporate headquarters of large business customers. A degree of coordination and harmonisation could be achieved through the use of Guidelines and/or Recommendations regarding the operation of such measures, whether issued by the European Commission or by BEREC.

The case for alleviating the administrative burden on **operators providing services to business customers** is even more pressing and straightforward to address. Interaction with stakeholders has revealed that a range of issues that are open to interpretation under the *EECC* impede their ability to introduce streamlined and cost-effective measures to address the following (and non-exhaustive) range of issues:

- The **details required to support an authorisation request** vary in terms of the detail and scope of information-gathering, regardless of the approach in the *EECC* that this information be kept to the necessary minimum.
- The failure to have a **comprehensive online filing system** across the EU Member States for authorisation requests is at odds with the EU's Digital Agenda goals, and the failure to have authorisation and compliance materials provided in anything other than the local language (at least without a translation into one of the working languages of the EU) adds another unnecessary burden to trans-border service providers.
- The methodology used by NRAs or Ministries to calculate **administrative charges for authorisations** differs significantly across Member States, as do the amounts charged (measured by reference to common characteristics).
- The **consumer protection obligations** regarding tariff information and transparency measures should be seen as having little or no relevance to sophisticated business users and, in the absence of an exemption from such obligations where business customers are involved, NRAs should at least be encouraged to exempt operators from such obligations.[54]
- The conduct of very differently focused **market surveys and statistical exercises** across Member States, despite the importance of NRAs being able to draw conclusions and to develop best practices on common themes.
- The significant differences between Member State practices as regards their **implementation of data retention and data intercept rules**, leading to significant spikes in compliance costs.
- The legal uncertainty generated by the significant **overlaps that exist between data protection rules, e-privacy obligations and cybersecurity regulation**, depending on whether an operator is acting as a provider of electronic communications or acting in some other capacity.

Possible Options

*(1) The Commission should actively **explore those areas of regulation where the physical presence of a connectivity provider is currently required in each Member State**, with a view to allowing them to provide the essential service through a centralised presence where technology facilitates such a* centralised role. *This right could be accompanied by proportionate self-reporting obligations in furtherance of Commission guidance on such matters.*

In order to assuage the security concerns of the security services of individual Member States, however, a reporting and cooperation protocol may need to be established between their respective security services. Given the growing number of security concerns that exist at a European level

[54] As has occurred recently in Italy – refer to AGCM Decision No.307/23/CONS of 5 December 2023.

already which require cooperation and coordination, that task should not be disproportionately cumbersome to implement.

(2) As a necessary adjunct to the harmonisation of the authorization process under the EECC, the Commission should explore a range of options that could be taken across the EU 27 to ensure that service providers wishing to provide cross-border business connectivity services are not confronted with legal uncertainty, delays in deployment and excessive compliance costs. To this end, we take the view that ***a less ambitious form of "passport" that is available in the financial services sector could be introduced to facilitate pan-European service provision****; this could take the form of a single standard authorisation application that could have a direct translation into the various languages of the European Member States. A multi-Member State* ***authorisation could thus be issued by a central authority such as BEREC*** *– acting with the authority of the Member States - to cover a bundle of services (comparable to what occurs in relation to the grant of multi-State patents).*

(3) As an alternative to the "passport" system advocated above, BEREC could be assigned to create a diverse ***range of commonly used forms*** *such as those used for authorization applications, statistical surveys, and expressing the methodology for calculating authorization fees. Even such a straightforward exercise could have a positive impact on the compliance costs currently faced by providers of cross-border business services. As such, it would have a positive impact on the creation of an internal market for communications services targeted towards business customers.*

(4) Services directed towards business customers should not be subject to the same onerous ***transparency and tariff information*** *requirements demanded of service providers to end-users, as they do not require the protection afforded under the consumer protection provisions of the EECC.*

7.2 Spectrum

A perennial problem in forging a comprehensive internal market for digital connectivity is the **difficulty faced in the allocation of spectrum on a pan-European or regional basis**. While it is understandable that Member States should wish to maintain their sovereign rights in relation to spectrum, and benefit from its valuation as a scarce resource, it is just as necessary that certain measures be adopted that will facilitate the provision of pan-European services, as this will greatly underpin Europe's ability to benefit from advances in the IoT environment. This means that Member States will need to play an active role in the creation of a regime that will accommodate trans-border service provision without the need for multiple interconnection relationships, that inevitably raise the cost of doing business.

Insofar as Member States could be convinced to designate a portion of their available spectrum bands to trans-border use, consideration could be given to whether they would be willing to designate a range of available spectrum bands to MNOs for identified cross-border business uses and for inter-institutional communications across borders. To this end, aside from the adoption of a more harmonised approach among Member States, **traditional State aids policy for broadband deployments and Important Projects of Common European Interest could also be modified to complement such changes in spectrum allocation.** Business users have historically been the most lucrative customer segment for the consumption of electronic communications services across

borders, with MNOs having identified this customer segment as the basis upon which cross-border services can satisfy existing demand. In setting aside a distinct set of 5G spectrum bands or portions thereof for cross-border business use, however, attention should be paid to ensuing that **existing spectrum allocations are not deprived of scarce already-acquired spectrum resources** through any such allocation.

The impact of other complementary policies involving the promotion of other Important Projects of Common European Interest (*e.g.*, regarding issues such as investments in trans-national **submarine cables** and in **data centres**), as proposed in the Commission's recently released *White Paper*, and the facilitation of network slicing possibilities compatible with Net Neutrality rules, should also be considered in tandem with changes in spectrum allocation policy. However, given the urgency in ensuring the protection of submarine infrastructures, **civil and military authorities need to intensify their cooperation** as a matter of priority in the sponsorship of new investments in submarine cables. For example, even when (urgent) security interests take precedence over competition concerns, the long-term impact of such measures on the market structure of the sector (or even the broader digital ecosystem) should be taken into consideration. For instance, facilities such as those used for information sharing for cyber or hybrid defence purposes should not become control *loci* which facilitate the undue exercise of power, either by operators or authorities.

Finally, there appears to be significant scope for an **increase in the greater shared or collective use of spectrum or for the systematic use of unlicensed spectrum**. Under the *EECC*, the promotion of the shared and collective use of spectrum is a policy that is a driving force for achieving the goals of the Code, including the promotion of competition, the creation of an internal market, and the generation of benefits to consumers and businesses.[55] That policy has been adopted by the RSPG in a series of initiatives.[56] To this end, a handful of multi-operator radio access networks have been created, with larger scale common use networks being made available in Member States such as Finland, Hungary, Denmark, Italy and Sweden. Nevertheless, despite these efforts to date, there is a general feeling that this avenue of cooperation to achieve more optimal spectrum use is just the start of a "work in progress" that needs to be expanded.

Possible Options

(1) To the extent that such an approach would be consistent with the efficient use of 5G spectrum, encourage Member States to ***coordinate the allocation of certain spectrum bands for use by MNOs for the benefit of multinational business customers and cross-border institutions****, encouraging their cooperation through the Radio Spectrum Committee and the Radio Spectrum Policy Group in doing so.*

(2) Use the ***Important Projects of Common European Interest (IPCEI)*** *vehicle in State aids policy as the basis upon which Member States can* ***be encouraged to vacate certain spectrum bands for cross-border use. That legal vehicle can also be used to further other projects which foster greater***

[55] Refer, for example, to Article 2(2), Article 45(2) and 46 of the *EECC*. This can be achieved through one of three avenues, namely: (i) a Collective Use of Spectrum (CLS) licence-exempt scenario or under a general authorisation model; (ii) under a Licensed Shared Access (LSA) scenario where users can be granted individual rights to provide discrete services in a particular frequency band; or (iii) a combination of the above two scenarios.

[56] For example, refer to the 2020 Working Programme and the 2021 Opinion on Spectrum Sharing. Refer also to the older Commission Communication on promoting the shared use of radio spectrum in the EU, COM/2012/0478.

***European market integration, such as the promotion of submarine cables**. Note, however, that efforts should be made to streamline procedures under the IPCEI vehicle, as it is arguably too time-consuming to implement for individual projects which need to be implemented quickly.*

*(3) Develop a **more ambitious and coherent policy framework for shared use and access to unlicensed spectrum**, as this is an area of potential great promise in reducing scarcity. To date, neither the technology nor the licensing regimes necessary for its effective implementation have been adequate on a pan-European level.*

7.3 Satellite communications

Traditional communications satellites are geostationary and have been in orbit for more than 50 years. **GEO satellites** weigh more than 1000kg and operate 36,000 kilometres above the earth. These satellites remain in a fixed position relative to any position. Despite the Earth's orbit, this allows ground-based antennas the ability to point directly at the satellite, in a fixed position.

In contrast, **Low Earth Orbit** (**LEO**) satellites are miniaturized, orbiting versions that operate between 500 and 2000 kilometres above Earth's surface and weigh under 500kg. Due to a LEO´s low orbit, latency is significantly reduced as the satellite is better positioned to quickly receive and transmit data. Unfortunately, this also creates a smaller coverage area, which means that LEO satellites continuously hand off communication signals and traffic across a constellation of satellites. This ensures seamless, wide-scale coverage over a pre-defined geographical area.

However, it has only been a relatively recent phenomenon that satellite has become native to the 5G standards suite. LEO satellites will play a key role in extending cellular 5G networks to air, sea and other remote areas not covered by small cell networks. For the end-user, satellites offer a seamless extension of 5G services from urban areas to airplanes, cruise liners and other vehicles in remote locations. In addition, IoT sensors and M2M connections on farms and remote worksites can also capitalise on the **wide coverage areas** offered by 5G satellites. As a stand-alone broadband service, however, the relatively expensive initial investment in acquiring a satellite dish means that it is arguably still too expensive for widespread consumer take-up other than in areas with poor broadband coverage. Falling subscription rates, however, would render satellite broadband services comparable in price to many fixed broadband offerings.

Integrating satellites with 5G infrastructure improves the Quality of Experience (QoE) of high-capacity applications. By intelligently routing and offloading traffic, satellites save valuable spectrum resources and improve the resilience of each network. In the event of a natural or man-made disaster where 5G infrastructure is damaged, satellite networks can take over and keep the network alive with an important role to deliver critical communications services during emergencies. Already, many telecommunications operators are **partnering with satellite firms to extend 5G services** in remote areas. There is currently one leading LEO constellation (Starlink), while another is clearly being planned (Amazon's Kuiper), with several others being at various stages of development. Nevertheless, there exists a risk that this new frontier will be heavily concentrated in the short term (including strong competitors such as Viasat and Eutelsat's OneWeb), although excess capacity over demand may also be a mitigating factor in the early stages of deployment.

Possible Options
(1) At this stage of its development, it is too early to predict with any certainty whether satellite offerings will be deemed to be a substitute, as opposed to a clear complement to other network broadband offerings. It is also too early to predict whether the broadband offerings made possible by such satellite communications will ever grow to such an extent as to require their incorporation into some form of asymmetric regulation (including the proposed 'bottleneck' regulatory framework explored above). Having said that, absent the security risks that they might face from sabotage and interference in politically volatile circumstances, satellites provide a source of ***potentially untapped potential when it comes becoming a major complementary provider of IoT cross-border services alongside mobile operators****. Satellite services also contribute towards the development of a more integrated European policy of network resilience and security, especially given their complementary role to mobile communications services.*

Annex: Competition Law in the electronic communications sector

General policy orientation

At a high level, the Commission's approach to competition law is now much more closely focused on **examining short-run effects on consumer welfare** than it was in the early years of competition enforcement. This has two consequences. The first is the increased role that economic analysis plays, as seen by the ever longer and more granular analysis in the Commission's merger decisions. The second is that wider policy considerations have played a significantly less important role than in the past. Agreements are no longer authorised when they serve to contribute to other policy goals, as was the case when the Commission allowed crisis cartels in the 1970s.

Some commentators have claimed that the Commission's use of commitment decisions and more intrusive remedies in the past 20 years reveals a more policy-oriented focus to competition law.[57] The policy being embraced is to open markets to competition: new techniques may be used, but the primary objective remains to complete the internal market and to keep markets competitive. That policy is narrowly cast but is delivered with innovative solutions. The 4-to3 mobile sector **merger decisions summarised in Table 1 below** exhibit this pattern well: the Commission retains a short-run consumer welfare analysis and accepts commitments which, in its view, are likely to allow the emergence of additional rivals to the merged entity.

However, **in recent years this policy direction has come under pressure**. For example, with respect to sustainability agreements, the Commission had to respond to demands by industry to take a clear stance on how far agreements that pursue sustainability goals might be authorised. In response, it has made some material concessions in its 2023 *Guidelines on Horizontal Agreements*. More generally, the Commission as a College is aware of the importance of using its legal tools to promote EU industry. Even in a technical document like the recent *Market Definition Notice*, the Commission observes that the enforcement of competition policy should address market failures, "*thereby contributing to the twin green and digital transitions and the resilience of the single market*."[58] The key issue that arises therefore is the extent to which the Commission may use this policy-directed approach to modify its analysis of markets to accommodate longer term consequences which promote other relevant policy considerations. The question is therefore whether we can expect a departure from the prevailing enforcement paradigm in light of current, more strategic priorities, with a more deliberate emphasis on industrial policy.

Merger control

The *Horizontal Merger Guidelines* relied upon by the Commission date back to 2004. Within the framework of assessing **unilateral effects** in the absence of a finding of individual dominance (which is the principal scenario encountered in telecommunications sector mergers), much of the economic

[57] P. Ibanez Colomo, The New Competition Law, Bloomsbury Books, December 2023.
[58] *Market Definition Notice*, at para 3, with reference to "*A competition policy fit for new challenges*", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2021) 713, 18 November 2021, page 6.

analysis rests on insights that have been developed after that date. A review of the *Guidelines* seems overdue, irrespective of whether a policy change occurs along the lines discussed in Section 1 above.

With respect to telecommunications sector mergers, what we see is an increasingly sophisticated set of measures to determine the competition risk, but at times less clarity as to the theory of harm that is driving the analysis. Some clarification in this context is necessary even if one retains a narrow policy focus of identifying only competition risks based on a short-term consumer welfare standard.

First, a re-thinking may be required of the emerging competitive dynamics that are foreseeable in the way that electronic communications services are provided. In light of these new **technological developments**, which disassociate the market power of an operator from the underlying network assets which they have deployed, is it still realistic to insist on the short-term emphasis that four MNOs are necessary to maintain competition in each national Member State market?

For example, in a number of decisions relating to other sectors the Commission has elaborated theories of harm that look also at long term effects. In particular, in *Dow/du Pont* the Commission elaborated an innovation theory of harm which considers the impact of a merger on *future* research and development and *future* product market competition. The conditions for identifying this competition risk are very particular, with the Commission assessing market contestability, the role of innovation and the role of intellectual property rights protection.[59] From one perspective, the innovation theory of harm rests on the fundamental analysis used for all kinds of anti-competitive effects, namely: does the merger remove a rival who would likely have remained a strong competitor? However, it can be seen to be simply asking the same question by reference to incentives for future innovative conduct. Yet from another perspective, the message that may be taken from this approach is that long term effects are important in certain industry sectors, and they might need to be taken into account when considering mergers between MNOs: might their incentives be affected by new technological developments which mean that the risk that they would harm competition is reduced? Perhaps such a longer-term analysis of markets in the telecommunications industry is also warranted to explore the likely impact of their future conduct.

Second, it also worthwhile to revisit a more classical debate, which is the role of **efficiencies** in merger control. While it is well understood that the European Commission is open to efficiency defences as a matter of general principle, these have rarely been successful in practice. In part, this may be because the legal standard that needs to be satisfied may not have been set correctly. As a starting point, the efficiency defence is set out as a means of rebuttal and not as a defence. In other words, the parties to the merger have to prove that the merger will *not* cause the anti-competitive effects that the Commission alleges in its analysis.

According to the *Horizontal Merger Guidelines*, proof of efficiencies will lead the Commission to authorise a merger when it is *"likely to enhance the ability and incentive of the merged entity to act pro-competitively for the benefit of consumers, thereby counteracting the adverse effects on competition which the merger might otherwise have."*[60] Put more bluntly, the theory of harm asks whether the merged entity will increase price, whereas the analysis of efficiencies asks whether the

[59] Case M.7932, *Dow/du Pont* 2018, Annex 4 contains a synthesis of the economic approach undertaken by the Commission.
[60] Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings [2004] OJ C31/5, para 77.

merged entity will cause prices to go down (*i.e.*, the benefit is couched purely in terms of consumer benefits). It is therefore *not* framed as a balancing exercise between two competing effects. This in effect makes it structurally impossible to run a successful argument that a merger can improve the prospect of investments because these positive effects *cannot* countervail the harm to consumers that would exist in the short term.

This approach to efficiencies rests on a deeply rooted commitment that competitive markets are the only source of innovation, but this may not be true for every industry and at every stage of that industry´s development. For example, let us consider a situation where there are four players in a telecommunications sector and a maverick is pricing aggressively. The maverick might be able to price aggressively because it has not invested in developing a full network and relies on wholesale access. Its conditions of market entry might also have been uniquely favourable, as occurred in Austria when Vodafone's network was sold to the new entrant for the modern equivalent of a "peppercorn".

A longer-term view might yield the result that the maverick cannot sustain its aggressive pricing policy in the absence of significantly increasing market share. There may thus be short term gains for consumers, but these will come at the expense of network investment. The reduced profits of the other three telecommunications providers mean they have no incentive to upgrade their networks, which ultimately puts a break on their ability to engage in future innovation. In this particular context, if the maverick is acquired by one of the other three operators, the result could be greater network investment, which would in turn raise the possibility of longer-term innovation taking place. Consumers would thus gain from the improved quality of the network, even if prices might rise in the short term. As its administrative practice stands at the moment, the Commission is unlikely to accept an efficiency rebuttal in these circumstances, however, where the merger has removed a maverick.

Moreover, on the issue of efficiencies, the Commission has required that the merger is the **least restrictive way of achieving the efficiency gains** (the merger specificity requirement). At times, the counterfactual relied upon is a scenario involving a network sharing agreement. However, this may be too optimistic: as we can see from the *Czech Network Sharing Case*,[61] the Commission carried out a very lengthy investigation before arriving upon a remedy that removed all of its competition concerns. More generally, from a strictly legal perspective, if the generation of efficiencies constitutes a rebuttal of the anti-competitive effects created by the merger, there seems to be no need for a proportionality requirement to be deployed because the merging parties have demonstrated that the merger causes no harm.

In sum, further reflection on the redesign of the way in which arguments regarding efficiencies are raised in merger reviews seems to be desirable. If the current efficiency rebuttal approach is retained, the requirement that efficiencies should be merger-specific seems to be unnecessary. By the same token, if efficiencies are re-calibrated as a means of making trade-offs between short-term losses and long-term gains, a different approach is required than that which is currently found in the European Commission´s *Guidelines* and in its merger decisions adopted to date.

NAME/COMMISSIONER	TYPE	DECISION/REMEDY	NOTES

[61] Case AT.40305 *Network Sharing – Czech Republic*, 2021/C 398/16, C/2021/7128, OJ C 398, 01.10.2021, p.24.

M.3916 **T-Mobile Austria/tele.ring (2006)** **(C/er Kroes)**	5 to 4	Phase 2 with commitments to create another strong player to replace the target	Only case where there is a single theory of harm.
M.4748 **T-Mobile/Orange** **NL (2007)** **(C/er Kroes)**	4 to 3	Phase 1 clearance with no commitments - Art 6(1)(b)	Para 35 conflates aspects of two separate theories of harm.
M.5650 **T-Mobile/Orange** **(2010) (UK market)** **(C/er Kroes)**	5 to 4	Phase 1 clearance with commitments designed to keep 3UK in the market as a competitive constraint.	MVNOs here are seen as a major force. This is also a largely unproblematic concentration.
M.6497 HUTCHISON 3G AUSTRIA / ORANGE AUSTRIA **(2012)** **(C/er Almunia)**	4 to 3	Phase 2 cleared with commitments to: a) divest spectrum to facilitate MNO entry b) share 30% of network to allow up to 16 MVNOs to enter	Last of the 3G cases, 4G LTE on its way. Starts with a clear theory of harm, but then has other elements. Two smallest MNOs merge. This seems to be the first case where DG COMP cites economic studies + relies expressly on the use of the UPP test.
M.6992 Hutchison 3G UK/Telefónica Ireland (2014) **(C/er Almunia)**	4 to 3	Phase 2 cleared with commitments to: a) facilitate entry of 2 MVNOs, one with an option to buy spectrum and climb the investment ladder b) commitment to continue network sharing with Ericsson so that it stays in the market	Annexes are included to develop the economic theory in more detail. UPP discussion in the Annex with much more detail: trend continues in later cases as there is a confrontation between the Commission and the

			parties on the details of the economic analysis. Efficiencies defence become more sophisticated from hereon. ** Commission undertakes empirical analysis hereafter to determine whether price increases followed earlier Irish and Austrian 4- to- 3 clearance decisions.
M.7018 Telefónica Deutschland/ E-plus (2014) (C/er Almunia)	4 to 3	Phase 2 clearance with commitments to: a) allow entry of 3 MVNOs by offering them network capacity b) divest frequency auctions to allow new MNO or a MVNO to climb investment ladder c) extend wholesale arrangements with MVNOs	Serious concerns about the efficacy of the commitments regarding next generation technologies (resulting in threats of litigation)
M.7419 Telia Sonera/Telenor (2015) (C/er Vestager)	4 to 3	Abandoned by the parties after Phase 2 commenced	Commission expected a remedy that would create a fourth MNO, but parties were unwilling to make such commitments
M.7612 Hutchison 3G UK/Telefónica UK (2016) (C/er Vestager)	4 to 3	Blocked	Decision quashed on appeal by the General Court; renvoi to the General Court in 2023 after the ECJ upheld the Commission's Decision.
M.7758 Hutchison 3 Italy/WIND/JV (2016) (C/er Vestager)	4 to 3	Phase 2 clearance with commitments to create a fully-fledged new MNO (Iliad)	From this case onwards, it seems that the Commission no longer considers MVNOs to be a competitive counterweight to MNOs.

			Internal communications did not support an efficiency-driven rationale for the merger.
M.8792 T-Mobile Netherlands/Tele2 Netherlands (2018) (C/er Vestager)	4 to 3	Phase 2 clearance with no conditions	Small market share increment and weakness of Tele2 NL highly relevant to analysis. First time an efficiency defence is made out but is irrelevant in the final analysis, as merger is cleared for other reasons. Internal communications supported the efficiency arguments of the parties.
M.10475 United Group/Wind Hellas (2021) (C/er Vestager)	4 to 3	Unconditional clearance	No overlap in mobile telecommunications services, combined market share between 10 and 20%, minimal overlap in other markets
M.10896 Orange/MasMovil (2024) (C/er Vestager)	4 to 3	Phase 2 with commitments of spectrum divestiture and other remedies to benefit an up-front new entrant MNO.	New entrant was not a high-profile buyer with an established track record.

cerre Centre on Regulation in Europe

END-USERS REGULATION

ANTONIO MANGANELLI

Executive Summary

This paper focuses on end-users regulation for the electronic communications industry and deals with the main **demand-side issues - i.e., consumer protection, net neutrality and universal service - trying to build a coherent narrative and approach for their coordinated rethinking**. In doing this, market and technological evolution are considered, primarily, the creation and consolidation of an extended value chain and digital ecosystem where a much wider set of players interplay. This analysis starts reckoning that **pro-competitive and pro-consumer EU electronic communications rules have benefited consumers, much more than in other jurisdictions**. Notwithstanding, the analysis clarify that each sector-specific demand-side regulation has an impact on market efficiency and that neglecting it could lead, in time, to distortions and unintended outcomes.

This is particularly relevant for consumer protection, as one of main aspect to consider is whether horizontal legislation could be sufficient to address demand-side issues. The paper advocates for a **streamlining of the sector-specific consumer rules in order to rely more on horizontal legislation**. This is mainly for those provisions concerning information requirement for contracts, and, for certain aspects on which competition has developed, also rules about contract duration and termination. The paper identifies a need of **higher harmonisation at EU level of the remaining sector-specific rules**, as well as harmonised regulation, under a functional approach, of all interpersonal communications services. It is also identified an overarching need to move from a regulatory definition of minimum quality standards for consumer protection, which comes with pure price competition, to a **consumer-empowerment approach supporting an enhanced quality competition**. Finally, it seems necessary to focus on **easiness to switch** (rather than actual switching and distribution of market shares), while, at the same time, those unengaged consumers who are not directly reached by the positive effect of competition and liberalisation should be further empowered. This could be done by defining some nudging/regulatory mechanisms to allow and facilitate them to subscribe a better offer among those that the same provider supply to its engaged users.

As for the efficiency consideration, overlooking the economic impact of current Open Internet Access Regulation is identified as one of the main problems regarding the implementation of Net Neutrality rules in Europe. This is coupled with the significant technological and market changes having happened in the last few years within the extended digital ecosystem. These evolutions transformed the largest Content Access Providers (CAPs) market position both in terms of countervailing power and their ability to influence end-users' internet experience. In this context, the paper advocates for a **net neutrality approach, embracing the 'proportionality' principle as well as having a systemic perspective** and thus reframing the existing partial and asymmetric approach vis à vis the different actors in the digital ecosystem. One of the main drivers for the new approach should be to avoid that net neutrality rules inhibit the ability of telecom industry to fully deploy capabilities of new technologies. A first step in this direction would be to **update and clarify at the EU level an interpretation of the Open Internet Regulation which takes into account technology and market evolution**. A second step would be grounded on a more radical rethinking, by allowing more flexibility and freedom for quality differentiation, as for premium quality services, as well as for zero-rating offers, both as 'class-based offers' and 'content-specific retail offers', yet only when it is the end-user choosing for such a differentiation. This could be done by introducing an application-agnostic 'anchor product' with a minimum QoS and which all users may choose. This **consumer-empowering approach**

to net neutrality could strike an effective balance, guaranteeing a freedom of choice, without over-restricting the economic and commercial freedom of companies. Finally, the paper looks at those situations in which network congestion could originate, advocating, in those circumstances, either for more freedom for of managing traffic or for mandating those CAPs (co-)causing congestion to contribute to network upgrades.

Indeed, network capacity is extremely important for the open internet objectives as well as for wider societal benefits. That's why challenging connectivity targets have been defined, as a future-proof EU industrial policy. Those targets assume that positive externalities derive from very high-capacity networks deployment, which, in turn, justify the extensive public subsidies programmes that have been tabled and implemented. This overall policy approach is clearly, yet not formally, setting a forward-looking ambitious universal service policy. Next to this, it stands the current universal service regulation that has a backward-looking approach. This striking divergence seems to call for an in-depth assessment about a **redefinition of the universal service, to be coordinated and consistent with industrial policy and connectivity targets**, and the existing state aids programmes. Under this perspective, an effective solution could be the establishment of a **connectivity fund**, where public funding (state aids) could flow and to which all players in the wider digital ecosystem could contribute, under a principle of proportionality, as an alternative or complement to public fundings.

1. Introduction

"End-Users regulation" is an ambiguous locution, often defined by contrast with "economic regulation". In those markets where competition cannot completely deploy its beneficial effects, "**economic regulation**" refers to legal obligations imposed on the supply-side, to firms (usually, with significant market power) in order to promote competition and the well-functioning of the markets (or mimicking a well-functioning). Thus, economic regulation aims to increase social and consumer welfare indirectly, via competition enhancement and market interactions. **End-users regulation** also refers to legal obligations imposed to firms, but, usually, it aims at increasing consumer welfare directly and pursuing consumers interest without using market competition as a tool. Therefore, both economic regulation and end-users' regulation are generally supposed to have positive effect on consumers. Namely, as far as the EU regulatory framework is concerned, both pro-competitive supply-side rules (i.e., access and interconnection regulation) and pro-consumer demand-side rules have resulted **in a larger share of the market value to benefit consumers, compared to other jurisdictions**.

Economic regulation always has (or should have) efficiency objectives, even if regulators are often called to address some untrivial trade-offs between different kind of efficiencies (productive vs allocative as well as static vs dynamic). By contrast, end-users regulation is often considered unrelated to efficiency objectives but generally oriented to social fairness and redistributive aims, because it tries to pursue the interests of consumers - who usually are the weaker parts in market negotiations and transactions.

This simplistic distinction between end-users regulation and economic regulation are neither clear-cut nor always accurate. For example, fairness objectives can be indeed identified in consumer protection regulation, which aims to directly rebalance the greater bargaining and informational power enjoyed by large corporations and thus the possibility of making a free choice that is not conditioned by heavy contractual constraints or switching costs. However, these rules also have a pro-competitive effect and thus an efficiency rationale, in that they allow consumers to play their disciplining role in business and the market. Moreover, all demand-side rules aiming to provide consumers with clearer information directly assess a 'classical' market failure, i.e., asymmetric information.

Likewise, fairness and redistributive objectives may be related to the imposition of generalised supply or price control obligations on companies that offer 'essential' products and services. Even in this case, however, efficiency profiles arise from the fact that these goods and services (of general interest) are often associated with positive externalities whereby private benefits are less than social benefits and therefore, in the absence of public intervention, there is sub-optimal production and consumption of those goods and services.

As described in the following, **end-users regulation could be either horizontal (i.e., covering all sectors and industries) or sector-specific (i.e., specific to a certain sector)**, whereas economic regulation is prominently sector-specific as it is inherently related to the specific economic features of each distinct market and industry. When end-users regulation is designed as sector-specific and tasks are assigned to sector-specific economic regulators (and not to public actors with general purpose, e.g., ministries or ministerial agencies, or horizontal consumer authorities), their action is always associated with greater attention to efficiency and well-functioning of markets. In other words, sector-

specific end-users regulation is often designed to pursue "social aims", yet minimising any distorting impact on competition and market efficiency, thus, when possible, working in a synergic way.

This paper focuses on end-users regulation for the electronic communications industry and deals with the main demand-side issues, trying to build a coherent narrative and approach for their coordinated radical rethinking.

The paper is divided as follows:

- Consumer protection / consumer empowerment (section 2);
- Net neutrality (section 3);
- Universal service and social tariffs as well as subsidies for investment deployment and take-up (section 4).

As said, each of these policies has (or should have) also efficiency rationales and the competitive impact in the playing field should be always taken into consideration. This is even more relevant in a context of increasing interdependences between the ECSN providers and other actors active in what could be considered an extended digital network and services value chain. Of course, a radical rethinking of regulation should not overlook this process, on the supply-side as well as for the definition of the demand-side rules.

For each of those policies the paper describes the current EU regulatory approach and framework, aiming to generally analyse how the market trade-offs are addressed, what is their capacity to result in efficient or fair market outcomes, as well as the need and possibility for introducing a different approach. In doing this, the paper always highlights what are the main issue to look into and to assess and what is a general direction to aim at.

Giving the complexity of the issues at stake and the need of an overarching coherent vision, the paper does not provide detailed recommendations, but rather a direction toward which policy making and regulatory activity should be oriented, while at the same time shaping and contributing to the "Overview and Recommendations paper".

2. Consumer Protection: From Fairness to Efficiency

2.1 Consumer Protection and Empowerment

Consumer protection at the EU level (not only in the context of regulated markets) has traditionally been marked by legal rather than economic considerations. This is mainly because consumer protection policies initially focused [62] on health and product safety issues, thus covering extremely sensitive issues that were considered not to be subject to economic considerations.

These rules mostly identified consumer as the weaker party in a bargaining and contractual relationship and therefore, in light of fairness and social justice, aimed to level the contractual imbalance by implementing a quasi-redistributive function and preventing the stronger parties from appropriating the largest share of the benefits of the exchange.

Moreover, EU consumer policy started almost two decades before the liberalisation of public utilities, when, obviously, in those markets there was no possibility of choice outside the monopolistic operator, so consumers were not required to have knowledge of the market, of the terminology in use and, above all, were not required to know how to compare offers of different operators, evaluating costs and benefits. Following liberalisation, this knowledge and awareness is instead required, not only for the private interest of the single consumer, yet also for the well-functioning of the market and the overall consumers' welfare. Indeed, as anticipated, in standard economic theory, consumers play a pivotal role in competitive markets, because consumers' free choice among alternative options in the market is the ultimate force that disciplines market power and introduces the appropriate incentives for firms' efficient decisions.

Progressively, policy makers and regulators started to dedicate specific attention to the role of **consumers as a key for market well-functioning by developing so-called *demand-side liberalisation policies***. These policies were aimed to complement pro-competitive rules active on the supply side by empowering consumers and thus enhancing the competitive pressure on businesses from the demand-side, rather than merely creating legal protection for individual rights.

Generally speaking, empowered consumers are those: (i) aware of the providers and offers available on the market as well as their prices, characteristics and quality, when making a choice; (ii) aware of the service provided, in terms of quality and any "hidden" costs, during the provision of the service; (iii) having the possibility to withdraw free of charge from a contract or obtain a refund when services do not work as expected; (iv) have the possibility to change operator without incurring excessive costs.[63]

Today's consumer economic policies are built on those two paramount objectives:

[62] See Resolution of the Council of the European Communities of 14 April 1975 on a preliminary programme of the European Economic Community for a consumer protection and information policy, Official Journal [1975] EU C92/1.
[63] European Commission (2011) Staff working paper: Consumer empowerment in the EU - SEC (2011) 469 fin.

1. to directly protect consumers, acting in their interest and sometimes (paternalistically) choosing on their behalf;

2. to empower consumers by removing obstacles to the consumer free, rational, and informed choice, thus allowing them to play a disciplining role for companies' behaviours in the market, and thus enhancing competition.

A general distinction often applied is that, in principle, consumer protection is agnostic *vis a vis* the competitive structure of the market, so that those rules can be applied indifferently in a monopolistic situation as well as in a competitive market – that's why for most of markets the same (horizontal) rules apply exclusively; differently, consumer empowerment is usually in a two-way relationship with competition enhancement. Indeed, on one side, consumer empowerment is a competition-enhancing tool and, on the other side, in order to have substantially empowered consumers (that can exploit their power), it is necessary that a certain intensity of competition is in place on the supply side. Furthermore, market competition can (and should) involve quality (and not only prices), so potentially enhancing the quality of contractual terms and customer service (for those transactions entailing durable commercial relationships).

Nevertheless, this distinction between consumer protection and consumer empowerment is not always clear-cut, and it can entail challenging regulatory choices and balancing assessments: e.g., protecting consumers through excessive forms of paternalism, especially in competitive markets, would end up not only neglecting their rationality but even risking "producing" "lazy" consumers who renounce to engage with companies, seek information and make the most out of the information and experience available. On the other side, empowerment cannot be effective without a certain level of protection, a safety net, especially for certain categories or groups of consumers (e.g. 'vulnerable' ones), who need to be more openly and extensively "protected" as they are not able to engage on an equal footing with businesses, even under an extensive information disclosure regime, and therefore are not able to fully enjoy the beneficial effects of market liberalisation and competition enhancement.

As a matter of fact, those **consumers in need of "more protection" may well have different kinds of "needs"**. Mainly, three different categories can be considered: (i) non-sophisticated/ non-engaged consumers; (ii) consumers with low income and willingness/capability to pay, (iii) physically impaired consumers/minors.[64] The first category is the most interesting, under a consumer empowerment viewpoint, since it is composed of consumers that could play a role in the well-functioning of market, yet they are uneasy to be empowered; whereas policy actions in favour of categories (ii) and (iii) have clearly redistributive/fairness rationales and outcomes (and this paper will incidentally dial with (ii) in the universal service section of this paper).

2.2 Current EU Regulatory Approach

The EU adopted both cross-sectoral (horizontal) pieces of consumer legislation and sector-specific legislation, among which this paper mainly focuses on those for electronic communications services.

[64] Of course, those different categories could overlap, and disadvantages reinforce each other, for example, non-engaged consumers may be also low income ones, yet not necessarily.

The main cross-sectoral acts include the Directive on unfair contract terms, adopted in 1993,[65] the Directive on unfair commercial practices, adopted in 2005[66], and the Consumer rights directive, adopted in 2011,[67] as amended in 2019 by the Directive on better enforcement and modernisation of EU consumer protection.[68] In addition, in 2020, rules were enacted in order to ensure that a representative action mechanism for the protection of the collective interests of consumers is available in all Member States (Directive 2020/1828/EU). By disciplining representative actions, this directive has given consumers the practical tools to effectively enforce their rights and get compensation.

Those directives have a twofold purpose:

1. an effective achievement of **market fairness**, by protecting the weaker party in the commercial relationships. Therefore, horizontal consumer policy approach is mainly on the consumeristic/legal side, thus tending to disregard the economic analysis of consumer behaviours.

2. the establishment of the **Internal Market** through a harmonisation of national consumer protection rules. These horizontal directives, covering all markets, have allowed consumer policy to achieve a high level of harmonisation, both in-country and cross-country. Indeed, an important positive aspect to consider about horizontal consumer protection rules is that they do not require each consumer to get a sound knowledge and understanding of several different sector-specific rules for each market, which could prove to be uneasy, especially for the less sophisticated consumers.

The Horizontal Consumer Directives

The ***Unfair Contract Terms Directive (UCTD)*** protects consumers against non-individually negotiated (standard) terms. Terms are deemed unfair when, contrary to the requirements of *good faith*, these contractual provisions are likely to cause significant imbalance in the parties' rights and obligations to the detriment of the consumer.[69] This outcome can be due to asymmetries of information as well as lack of expertise and bargaining power in relation to the contract terms.

The ***Consumer Rights Directive (CRD)*** harmonises national consumer rules about certain aspects of contractual relationship (i.e., pre-contractual information requirements, formal requirements for the conclusion of contracts, detailed rules regarding the consumer's right of withdrawal), which are particularly relevant for the telecom sector with specific regards of distance and off-premises contracts.

The main objective of the ***Directive on unfair commercial practices (UCPD)*** is to boost consumer confidence, by enabling national enforcers to curb a broad range of unfair business practices taking place before, during and after a transaction. The Directive identifies: (a) a list of specific illicit

[65] Directive 93/13/EC.
[66] Directive 2005/29/EC.
[67] Directive 2011/83/EC.
[68] Directive 2019/2161/EU.
[69] Art 3 UCTD.

practices;[70] (b) few general categories, i.e., misleading actions or omissions and aggressive practices;[71] and (c) a general principle under which is unfair any practice contrary to *professional diligence*.[72] A significant example for prevention of non-contractual barriers to switching regards "use of harassment, coercion and undue influence".[73] This provision prevents traders from imposing any disproportionate non-contractual barriers detrimental to consumers who wish to exercise their rights under a contract (including the right to terminate the contract or switch to another product or trader).

All horizontal consumer directives are principle-based so that provisions can have a wide scope and are sufficiently broad to catch the evolution of services, sales methods, and companies.

Despite their flexibility, the horizontal directives had to be updated in order to address digital and technological developments. This revision was enacted in ***2019 by the Directive on better enforcement and modernisation*** of consumer protection. This piece of legislation aimed to introduce a more effective enforcement, in particular involving sanctions (proportionality and increasing maximum fine) and remedies to which a consumer has access, such as monetary compensation, price reduction, or replacement.

On the substance, the so called "Omnibus directive" strengthened consumer's rights, when buying services, products, or digital content online, in order to maintain a similar protection online to that guaranteed in the world of physical shops. These new horizontal consumers' online rules mainly refer to transparency obligations placed on online traders and marketplaces.

Indeed, as the economy became more digitalised, digital markets and services no longer constitute (vertical) sectors of the economy but rather its very (horizontal) foundation. Therefore, a horizontal piece of legislation was needed and most digital-specific consumer protection rules have been properly allocated into those horizontal rules. As a mere example, one of the revisions of the "omnibus directive" concerned digital content and digital services provided with no monetary exchange (yet in implicit exchange of personal data), including them in an extended scope of the consumer rights directive, aligning it with the Digital Content Directive (2019/770/EU).

The ***Digital Content Directive (DCD)*** is another piece of horizontal legislation that sets common rules on certain requirements concerning contracts for the supply of digital content and digital services, in particular on: (a) the conformity of digital content or a digital service with the contract, (b) remedies in the event of a lack of such conformity or a failure to supply, and the modalities for the exercise of those remedies, and (c) the modification of digital content or a digital service. The application of this Directive to electronic communication services is explicitly excluded but for NIICS.[74]

[70] Annex I UCPD.
[71] Art 6, 7, 8 UCPD.
[72] Art 5 UCPD. 'Professional diligence' means the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity, art 2 h UCPD.
[73] Article 9(d) UCPD.
[74] Art 3.5.b, directive 2019/770.

Next to the horizontal directives, covering all sectors, a detailed **sector-specific legislation** is in force, placing consumers into the specific context of telecom markets. Indeed, the electronic communications regulatory framework has always promoted citizens' interest, as one of its main objectives, by "*ensuring a high and common level of protection for end-users through the necessary sector-specific rules and by addressing the needs, such as affordable prices, of specific social groups, in particular end-users with disabilities, elderly end-users and end-users with special social needs, and choice and equivalent access for end-users with disabilities*."[75]

Nevertheless, within the EECC, the other main regulatory objectives are also framed in light of end-users' interest, as NRAs must: "*promote the interests of the citizens of the Union, by ensuring connectivity and the widespread availability and take-up of very high capacity networks, including fixed, mobile and wireless networks, and of electronic communications services, by enabling maximum benefits in terms of choice, price and quality on the basis of effective competition, by maintaining the security of networks and services*." As mentioned, this is because sector-specific consumers' rules, assigned to economic regulators, must be as synergic as possible with objectives pursued by economic regulation.

As for the scope of the demand-side rules, the EECC focus on: (i) transparency and contract information: (ii) conditions and procedure for contract termination; (iii) switching and number portability.

As for **transparency and contract information**, electronic communications providers are asked to inform consumers in a clear, comprehensible, and transparent way about quality of the service, service conditions and prices to facilitate a consumers' well-informed choice and make it easy for them to compare between alternative offers and providers. This information must be supplemented by at least one independent comparison tool, which can be used free of charge to compare and evaluate different services in terms of price and quality of service performance. [76] In addition, the Open Internet access Regulation (OIAR)[77] provides that contracts for internet access services (IAS) must include, for fixed networks, explanation about the minimum, normally available, maximum and advertised download and upload speed of IAS; and for mobile networks, the estimated maximum and advertised download and upload speed of IAS.[78]

Specific provisions require that conditions and procedures for **contract termination** do not act as a disincentive for changing service provider. First EECC limits service contract duration to a maximum of 24 months. This limit can be made stricter at national level (this is the case for example in Denmark where the maximum duration is 6 months or in Belgium where end-users can terminate their contracts at any time, without compensation except for the period of the first 6 months). Moreover, some MS still maintain provisions set by article 30(5) of Universal service directive (repealed by the EECC) posing obligation to provide at least one 12-month offer (this is the case in Croatia, Italy, Germany, Netherlands, Poland, and the UK).

[75] Art 3(2)d EECC.
[76] Art 102 and 103 EECC.
[77] Regulation (EU) 2015/2120 laying down measures concerning open internet access and retail charges for regulated intra-EU communications.
[78] Article 4.1(d) OIAR.

Moreover, if the contract provides for an automatic contract extension, consumers are entitled to terminate the contract at any time with a maximum one-month notice period, as determined by national law, and without incurring any costs except the charges for receiving the service during the notice period. Similarly, end-users can terminate their contract without costs upon notice of pejorative changes in the contractual conditions proposed by the provider.[79]

Finally, ECCC regulate **provider switching** and number portability. In case of switching, providers must provide adequate information along the entire process and ensure the shortest transition time. In any event, continuity of service must be ensured, unless technically unfeasible yet not exceeding one working day. End-users can retain or port a number to another provider any time for one month after the date of termination, without incurring in any charge. Porting of numbers and their subsequent activation must be executed within the shortest possible time, on the date explicitly agreed with the end-user, and in any event not exceeding one working day from the date agreed.[80]

2.3 What to Look Into

2.3.1. Horizontal or Sector-specific rules?

EU demand-side rules applicable to electronic communications services come both from the horizontal legislation and the vertical sector-specific one. In general, **any sector-specific rule should be linked to a sector-specific issue which justifies a differentiated intervention**. A sector-specific issue could be motivated by a technical reason and/or also an economic reason that specifically characterise the market. This is because having sector-specific rules in place always bare some risks/costs, which should be justified by their specific need.

First, despite any fine-tuning, there is always some potential overlapping that could lead to legal uncertainty. In case of conflict between the provisions in the horizontal directives and rules regulating specific aspects of unfair commercial practices by means of specific sectorial legislation, the latter would usually prevail (according to the general principle: *lex specialis derogat generali*).[81] However, this antinomy resolution mechanism didn't avoid competence clashes between telecom NRAs and national consumer/competition authorities, in charge of the application of horizontal legislations. Of course, this risk is absent where the same public body is empowered to apply both pieces of legislation. However, in the great majority of MS this is not the case. In addition, sector-specific demand-side rules require each consumer to get a sound knowledge and understanding of differentiated set of rules, which is costly and could prove to be uneasy, especially for the less sophisticated end-users.

This does not mean that all sector-specific rules should be eliminated, rather than **this differentiation should be objectively justified by market specificities** (as this is the case for economic regulation, which is inherently related to the specific economic features of each distinct market and industry).Precisely for this very same reason, not necessarily vertical sector-specific rules should cover both consumer protection and consumer empowerment: generally speaking, the former, which is not related to the competitive structure of the market, could be tendentiously tackled by the horizontal

[79] Art 105 EECC.
[80] Art 106 EECC.
[81] Recital 10 and Art 3(4) UCPD.

rules, especially when they are devised in a principle-based fashion, as it is the case for the EU *acquis*. So, in this context, a first general assessment to do is whether some overlaps are still in place in areas where horizontal rules alone could ensure an adequate level of protection for consumers and whether sector-specific consumer rules (especially among those ones aiming at a legalistic protection of the "weak" party in a contractual relationship) are really necessary as a complement to horizontal consumer rules, in order to address specificities of the sector.

2.3.2. EU harmonised or nationally differentiated sector-specific rules?

Another important general issue refers to vertical level of legislation, i.e., centralised at EU level or decentralised at national level. As described, horizontal consumers' directives have a primary objective to harmonise Member States consumeristic legislations.

Indeed, this is also a general objective for the demand-side sector-specific rules within the EECC, which precisely finds its legal basis in art 114 TFEU, concerning the harmonisation and approximation of MS's legislations. At this aim, a general principle of EECC consumer rules is one of "maximum harmonisation", meaning that member states may not impose more (and obviously less) stringent provisions than those set out in the EECC (art 101.1). This principle is particularly relevant for the overarching EU objective to create a single internal market,[82] which is pursued by secondary legislation for electronic communications by developing common sector-specific rules and predictable regulatory approaches.[83]

Notwithstanding, within the EECC there are extensive derogations to this general principle: (i) previous stricter national legislations (art 101.2) were allowed until 21 December 2021 if in force before 20 December 2018, and more relevantly (ii) quite a few other derogations are possible. Some of them are specific to contract information on the consumption level and newly emerging issues (art 102.6 and 102.7) and are directly defined in the directive ; another number of specific derogation could be enacted by member states: 103.4 (distributing public interest information free of charge), 105.1 and 105.2 and 105.3 (shorter maximum contractual commitment period and notice of termination after automatic prolongation and longer period of possible termination after contractual conditions 'changes), 106.7 (penalties concerning not compliance with switching and number portability rules).

A regulatory assessment here would be necessary to understand **whether national differentiations of demand-side rules are somehow justified, weighting this justification against the consequent risk of an enduring fragmentation** of rules within the internal market.

2.3.3. Sector-specific protection should be limited to consumers or applied to all end/users?

Another aspect to investigate, which is related to the previous ones, is what kind of end-user needs sector-specific protection or empowerment. In this regard, the EECC generally distinguishes between (i) consumers, as those natural persons using or requesting publicly available electronic communications services for purposes which are outside their trades, businesses, crafts or

[82] Namely, art 26 TFEU.
[83] Art 3(2)c EECC.

professions[84] and more comprehensively (ii) end-users, as those natural or legal persons using or requesting publicly available electronic communications services, thus comprising also businesses, yet only those not providing public electronic communications networks or publicly available electronic communications services.[85]

Sector-specific rules in the EECC are **generally referred to all end-users** (as for the title III of the code: 'end-user rights'), especially for contract duration and termination, for example provisions at: (i) art 105.3, dealing with duty of information for providers and the end-user's right to terminate anytime a contract when an automatic prolongation is foreseen; (ii) art 105.4, related to notice period for changes in the contractual conditions and the consequent right to terminate the contract without incurring in further costs; and art. 105.6, which states that where an end-user has the right to terminate a contract, e.g., (i) and (ii) above, no compensation is due by the end-user other than for retained subsidised terminal equipment.

However, there are quite a few limitations in specific provisions: for example, the application of art 102 (dealing with info requirements for contracts) and art 105.1 (dealing with maximum contractual commitment periods), as well as art 105.7 (related to M2M communications) are limited to consumers and those end-users that are microenterprises or small enterprises or not-for-profit organisations. [86] A stronger limitation is established for the obligation to refund, upon request, any remaining credit after switching provider of a pre-paid service (art 106.6), which is applicable only to consumers.

To assess whether the current approach should be reconsidered, especially for provisions applied to all companies, any assessment should start form the consideration that consumeristic horizontal legislation applies only to 'business-to-consumer commercial practices'.[87] This consideration highlights that consumer protection rules specific for the EC sector have a wider scope than horizontal legislation (comprising also B2B commercial practices) and thus implying that in this sector also companies are considered to be in need of some form of protection and/or empowerment.

Again, this may be a plausible market situation, which should be anyway subject to an assessment/ justification and not taken as a mere assumption. On the other side, it should be also considered that softening such rules would result in leaving those companies not covered by any demand-side protection (obviously other than contract and commercial law). However, this is exactly the point to assess: do the electronic communications sector's specificities imply that companies buying services are in a weaker position vis-à-vis companies that provide those services?[88]

[84] Art 2(15) EECC.

[85] Art 2(14) ECCC. The code also defines 'users' as an even more comprehensive concept including consumers, end-users and those electronic communications network or service providers using or requesting electronic communication services from other providers, i.e., access seekers.

[86] As for the EU Commission Recommendation of 6 May 2003 C (2003) 1422, a micro enterprise has fewer than 10 employees (and an annual turnover below €2 million), while a small enterprise has fewer than 50 employees (and an annual turnover below €10 million).

[87] E.g., art 3.1 UCPD.

[88] As a matter of fact, this assessment is at the basis of most of the recent digital markets and services regulation. Namely, The Platform-to-business (P2B) regulation (regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services) and the Digital markets act (DMA) (regulation (EU) 2022/1925 on contestable and fair markets in the digital sector). Whereas such rationale is not clearly highlighted for the electronic communication sector.

Probably, the answer depends on the size the business end-user (and how much sophisticated it is), not to be in a weaker commercial position, as well as on the level and type of competition that has developed in the electronic communications market.

The first aspect (size of the companies) is considered by the Code, upon which the scope of its demand-side rules is differentiated - even if, often, without highlighting a clear rationale. On the contrary, the second aspect, as described in the following section, is completely neglected by the Code, which envisages demand-side and supply-side rules as completely independent and thus not considering competition as a possible driver for enhanced quality of contractual relationships.

2.3.4. Homogeneous or differentiated rules for interpersonal communication service providers?

The recent Commission's White paper on digital infrastructure focuses on the fact that "yesterday's separation between 'traditional' electronic communications networks/service providers and cloud or other digital service providers will tomorrow be superseded by a complex converged ecosystem. These developments raise the question whether the players in such converged ecosystem should not fall under equivalent rules applicable to all and whether the demand side (i.e. end-users and in particular consumers) should not benefit from equivalent rights"[89]

According to this vision, all the sector-specific demand-side provision (which would not be allocated in the horizontal rules) should be in principle extended to all services in this extended ecosystem. This would be especially true for those services that are potentially substitutes on the demand side, e.g., the Number-independent interpersonal communication services (NIICS)[90]

Therefore, another relevant aspect to consider about the current EECC consumer policy is that NIICS are very often exempted to comply with the EECC demand-side rules, i.e., art 103.2 and 103.4 (comparison tool, transparency, and publication of information), art 105.1 (and .3.4.5.6) (contract duration and termination), art 107 (treatment of bundled services), 110 (public warning systems) and interception obligations for national security issues. NIICS are instead subject to the provisions about contract information (art 102), and their inclusion in comparison tools assessments, when number-independent interpersonal communications services are on payment.

Therefore, under this perspective, it would be necessary to **assess, on one side, whether those networks and services which are part of this extended ecosystem should be subject to a harmonised regulatory framework, or there are justified reasons for a differentiated treatment**, considering anyway the impact that this may have on the competitive level playing field.

[89] European Commission (2024) White paper on How to master Europe's digital infrastructure needs? COM(2024) 81 final.
[90] EECC distinguishes the interpersonal communication services (ICS) into two sub-categories: (a) number-based ICS services, corresponding to the traditional fixed and mobile voice services, in which the service is connected with numbers in numbering plans , assigned by public authorities for the routing of traffic, and not only as a user identification, and (b) the ICS services independent of the number, provided by digital platforms (e.g., Skype, WhatsApp, Facebook messenger) where the number is only the user's identification and not assigned and used for routing operations.

2.3.5. Are there other (residual or forthcoming) consumers' issues?

Finally, it is necessary to assess whether there are other consumers' issues that has not been tackled by current rules or which originate from the evolution of new technological or market circumstances. As for the former, other demand-side issues to consider concerns whether the current empowerment approach has been completely effective or could be improved, while, as for the latter, it seems necessary to analyse the evolution of markets and technologies and ascertain whether new demand-side concerns are emerging, and, in case, whether sector specific rules should tackle them.

2.4 Policy Recommendations

2.4.1. Streamlining sector-specific consumer protection rules

As anticipated, sector-specific consumers' rules bare some risks/costs, which should be justified by their specific need. Therefore, a default setting should be to rely on horizontal consumer legislation, i.e., remove those rules from sector-specific legislation, unless there is a justified need for a sector-specific rule.

To identify which sector-specific demand-side rules to maintain, policy makers must ascertain **what rules are consumer-empowering and have efficiency-enhancing outcomes**. That is those provisions which:

1. are at the basis of the "demand-side liberalisation". Indeed, those provisions should be preserved in their sector-specific fashion as they represent a pre-requisite for developing competition in the market by giving consumers the substantial possibility to have a choice (likewise supply-side liberalisation gave formal possibility to consumers to have a choice). These processes are necessarily sector specific as they depend on the characteristics and economics of the markets;

2. are mechanisms to further enhance competition, not (only) in terms of price competition, yet (mainly) in terms of quality competition. Indeed, price competition is quite intense in the telecom markets (mostly in the mobile markets, and depending on the country, also in the fixed), whereas quality differentiation and competition is not equally intense (especially in consumer markets, while it is more developed for business' services). This outcome is important both for allowing consumers to get a better quality and better return for their money, and for moving away from a complete commoditisation process of EC networks and services.

These assessments should be performed by separately considering the different kind of pro-consumer rules, currently disciplined by the EECC, as previously described: (i) transparency and contract information: (ii) conditions and procedure for contract termination; (iii) switching and number portability.

Under this framework, it seems that (i) **provisions concerning information requirement for contracts[91] could be well covered by horizontal consumer rules**. Likewise, all those extensive additional consumeristic sector-specific rules not based on the EU legislation and developed at national level (with wide difference from country to country), concerning, for example, indirect price regulation, customer care/helpdesk, parental control, often imposed only on IAS and number-based interpersonal communications services. Some examples could be represented by legislations imposing (a) no-penalty for cancellation even within the binding maximum contractual duration or (b) a "human touch" on customer care/helpdesk activities, either completely excluding the possibility of a complete automatic service or even imposing a 'human-first' contact. As for these additional and fragmented demand-side consumer rules, also considering the objective of consolidation of the internal market, the EU framework should enforce a strict and effective maximum harmonisation approach, by eliminating the several possibilities to include additional or stricter provisions, currently available for Member States.[92]

On the contrary, technical provision regarding (iii) **switching and number portability[93] should be maintained** and covered by sector specific rules as those clearly are sector-specific issues regarding the systemic well-functioning of the markets (like the interconnection provisions) and eliminates substantive economic switching costs.

Differently, rules about (ii) **contract duration and termination[94] fall in a grey area**. These provisions could be partially covered by horizontal rules and, especially in a competitive context, could represent QoS parameters that could be considered by end-users in their choice, if correct transparency and signalling commercial mechanisms are put in place. On the other side, quite obviously, certain practices regarding contract duration and termination can artificially raise switching costs and create lock-in (which is a sector-specific issue because it depends on the intensity and type of competition in the market).

Therefore, the main question here is whether service providers also compete on these kinds of parameters and such competition is effectively giving consumers a differentiated choice. This is an assessment that could be performed periodically either by the EU commission or by national regulators, where a lack of competition on these parameters could trigger a sector-specific demand-side regulation that by default is not in place.

However, the "quality" of contractual terms could be a complex choice for consumers, especially the less sophisticated ones, particularly affected by the '*bounded rationality*'.[95] Indeed, consumers often do not factor in all the costs/benefits that a certain action implies, especially if they are not contingent, causing so-called *internalities* (namely, externalities that people impose on themselves).[96]

These effects are of course differentiated not only between different kind of consumers (sophisticated vs unsophisticated), yet namely between consumers and business end-users. Therefore, this aspect is

[91] EECC, Art.102.
[92] Indeed, a quite non-investigated source of regulatory failure and inefficiency is the 'populistic' consumer rules developed by national policy makers (especially in certain countries) to gain electoral consensus.
[93] EECC, Art.106.
[94] EECC, Art.105.
[95] That is the inability to have access to and assess the relevant information, and to even understand their own (intertemporal) preferences to maximise their own utility. De Streel, Sibony (2017).
[96] Allcott H, Sunstein C (2015).

pivotal also for the question related to the scope of demand-side rules, i.e., whether limiting those only to consumers or applying also to businesses. As described, currently, quite a few consumer protection rules apply to microenterprises, small enterprises, and for-non-profit organisations of any size. If it sounds fair and rational to extend to microenterprises the same protection that is granted to consumers, some differentiation should be started to apply to small enterprises and, namely, to large for-non-profit organisation. The fact that an organisation is for-non-profit does not imply that has not a countervailing buying-power and that is an unsophisticated end-user.

Moreover, as described, most of the provisions related to contract termination apply also to all businesses and enterprises. Some deep consideration should be specifically devoted on whether this extensive approach, should be reconsidered, for example by limiting this protection to small enterprises and small for-non-profit organisation. Furthermore, also an effective 'maximum harmonisation' should be strictly guaranteed, without allowing any differentiation at national level.

As for figures about comparability, a recent consumer survey undertaken by the EU commission highlights that most consumers (about 70% both for IAS – table 1, and mobile communications- table 2) find either 'very easy' or 'fairly easy' to compare services.[97]

Table 1 – Ease to compare Internet Access Services (2020).

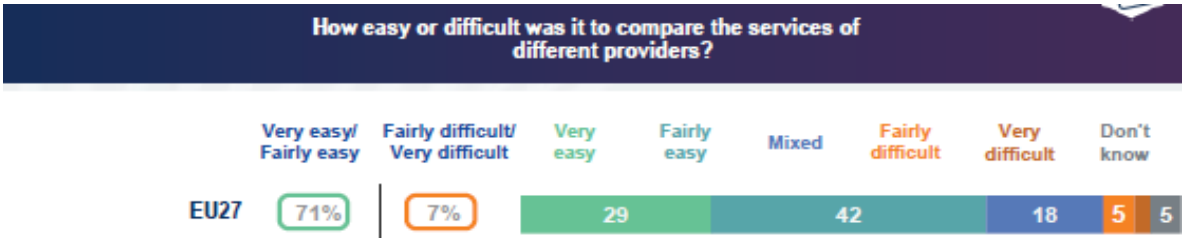


Table 2 – Ease to compare mobile services (2020).

Nevertheless, the more competitive variables are on the plate the more complex become the consumer's choice. Therefore, it seems necessary to devote some serious thinking about how improving and making effective the provision concerning the availability of at least one **independent comparison tool**, "which enables users them to compare and evaluate different internet access services and publicly available number-based interpersonal communications services, and, where applicable, publicly available number-independent interpersonal communications services."[98] Comparison tools are consumer-empowering instruments that aim to ease consumers' engagement by increasing information availability and reducing transaction/information seeking costs. As mentioned, they can increase the range of parameters assessed by users and thus, on one hand, give

[97] European Commission (2020) market monitoring survey 2020 – mobile services /internet provisions.
[98] Art. 103.2 EECC

a push towards quality competition and, on the other hand, increase the extension (rather than just the intensity) of competition, possibly making some consumer protection rules redundant.

According to a recent benchmark,[99] out of 13 EU countries scrutinised only 5 have a comparison tool powered by the NRA and another one is market-based. However, there are no clear data on the quality and effectiveness of such tools, which should be assessed, and which should be more and more be based on AI technology. One important question about comparison tool is why not to leave to the market the provision of such services, for which (considering the trend for digital platform services) there should be an increasing supply and a correlated increasing demand. Consequently, releasing regulators from these additional tasks, which are costly for them (and are costly also for telco companies in case they indirectly finance those services).

As a matter of fact, the current legislation does not impose a public provision, but just prescribes some compulsory features of independence, transparency, and openness that at least one provider must have. Of course, the existing "freely available" requirement pushes toward a public provision, which is not necessarily more effective and efficient compared to a regulated market-based solution. As often happen in the consumer policy, the current legislation seems to be animated by a mix of different kinds of "protection objectives": here the consumers' disadvantage is information asymmetry and a difficult comparability[100] and not an inability/unwillingness to pay.[101] Of course, in a scenario of market-based provisions the features of independence, transparency, and openness should be still prescribed by legislation, and maybe could be made mandatory for all providers. Yet, the "free provision" requirement should be removed to leave to providers a commercial freedom to set an effective business model.

2.4.2. Levelling sector-specific consumer rules

The subjective scope of sector-specific rules, i.e., what type of service providers should be disciplined, is a crucial aspect for the demand-side rules in the electronic communications, both in terms of end-users 'rights and in terms of competitive level-playing field. In this regard, the Commission's White paper proposes that the sector-specific demand-side provision (which would not be allocated in the horizontal rules) should be in principle **extended to all services that are potentially substitutes**, e.g., NI-ICS.

It is therefore necessary to assess whether this extension has a sound economic and regulatory meaning.

Direct switching costs (or multihoming) for online messaging services are usually very low or effectively zero; moreover, most services do not imply a monetary transaction for users, so the risk of consumer detriment is perceived as very low. Nevertheless, on one side, online messaging services, likewise other platform services, are characterised by extensive direct network externalities which

[99] Cullen International benchmark, February 2024, conducted on 13 counties (Belgium, Czech Republic, France, Germany, Ireland, Italy, Netherlands, Poland, Portugal, Slovakia, Spain, Sweden, United Kingdom).
[100] Compared to other markets, objectively, EC services can be more difficult to compare. This is not because the classical ex-post asymmetric information on the result or on the provider effort, but an ex-ante asymmetric comparative information about what the consumers are buying and whether relative prices differences are justified by differences in what they are buying.
[101] Anyhow, digital platform services often spontaneously assume two-sided business models where end-users receive free or low cast services.

(absent interoperability obligations) represent non-monetary switching costs.[102] On the other side, a consumer harm could be related also to data, not in terms of violation of data protection rules, yet considering the economic value of data transactions (which is already explicitly recognised in the EECC).[103] Moreover, it is often underestimated that most of demand-side obligations originates (opportunity) costs for companies and may well have an impact on level playing field between substitutes services.

Nevertheless, a general principle **of extension of consumer empowerment rules to NIICS must ensure a correct interplay with their regulation within the Digital Markets Act** (DMA). As well known, the DMA qualifies NIICS as core platform services and subject to its obligations when provided by a digital platform designated as gatekeeper. Indeed, one of the objectives of the DMA is to enhance fairness for end-users, which could be very close to a general consumer protection/empowerment rationale. In particular, NIICS are subject to interoperability obligation[104] which soften the regulatory asymmetry within the EECC (while by default only number-based ICS are subject to a symmetric interconnectivity obligation) and address some substantial lock-in issues for users given by net effects.[105] Moreover, the bundling of messaging services with other core platform services is tackled by the DMA, too.[106]

However, it is also to be considered that, due to its other objective, i.e., contestability, the DMA is an asymmetric regulation and thus imposed only on gatekeeper NIICS - currently WhatsApp and Messenger. Whereas consumer rules in the ECCC are symmetric and therefore applied to all providers.[107]

Therefore, an overturn of the current regulatory approach, based on the aprioristic and rigid exclusion of NIICS, should be considered. As a matter of fact, a "functional approach" is already enshrined in the EU code and should be effectively implemented: "the EECC adopted "a future-oriented definition of electronic communications services … build on a functional approach … [as] from an end-user's

[102] Manganelli A, Nicita A (2022).

[103] "Electronic communications services are often supplied to the end-user not only for money, but increasingly and in particular for the provision of personal data or other data. The concept of remuneration should therefore encompass situations where the provider of a service requests and the end-user knowingly provides personal data within the meaning of Regulation (EU) 2016/679 or other data directly or indirectly to the provider. It should also encompass situations where the end-user allows access to information without actively supplying it, such as personal data, including the IP address, or other automatically generated information, such as information collected and transmitted by a cookie. In line with the case-law of the Court of Justice of the European Union (Court of Justice) on Article 57 TFEU (16), remuneration also exists within the meaning of the TFEU if the service provider is paid by a third party and not by the service recipient. The concept of remuneration should therefore also encompass situations in which the end-user is exposed to advertisements as a condition for gaining access to the service, or situations in which the service provider monetises personal data it has collected in accordance with Regulation (EU) 2016/679." (recital 16 EECC).

[104] Art 7 DMA.

[105] Possible interconnection obligation for those number-independent interpersonal communications services which would reach a significant level of coverage and user uptake is foreseen where end-to-end connectivity between end-users would be endangered (art 61 (2) c EECC). This provision is subject to a vertical coordination mechanism, requiring a Commission decision outlining what measures can be taken by NRAs. This obligation has never been triggered so far. Moreover, this obligation, differently from interconnection obligation for NBICS, is an asymmetric regulation as it can be imposed only on key providers with a significant level of coverage and user uptake (designated under the EECC). See BEREC report on interoperability of Number-Independent Interpersonal Communication Services (NI-ICS) – BoR (23) 92.

[106] Art 5.7 and 5.8 DMA. Similarly to what art 107 EECC impose to number-based ICS.

[107] See BEREC Report on the interplay between the EECC and the EC's proposal for a Digital Markets Act concerning number-independent interpersonal communication services – BoR (21) 85.

perspective it is not relevant whether a provider conveys signals itself or whether the communication is delivered via an internet access service."[108]

Consistently with what recommended for the overall electronic communication services, periodic market assessments performed by the EU commission or NRAs should assess whether specific NIICS generate network externalities (e.g. in the form of switching costs) or data exploitation, thus inducing consumer detriment that is not remedied by other regulation (like DMA or DCD). This would trigger a sector-specific demand-side regulation that by default is not in place. Surely, a **higher coordination** of DMA and EECC for NIICS is necessary, both on the demand and the supply side, as well as a coordination with the Digital service and content Directive. Finally in the light of a converging/converged ecosystem possibilities of vertical/horizontal integration and bundling of services is foreseen to be rapidly increasing in the next future, for example also the inclusion of cloud in the EECC scope and thus the coordination with the remaining EECC demand-side provisions and also with the Data Act[109]).

Finally, it is extremely important noting that these actions are discussed in a scenario made of sector-specific rules. Of course, the more consumer protection rules would be based only on horizontal legislation, the more harmonisation, levelling and coordination problems would be tackled to the root.

2.4.3. Facilitating and incentivising competition on quality

Another important issue to assess for a revised regulatory approach is **how much the current demand-side policies are providing incentives and steering the market toward an enhanced quality competition rather than (only) price competition**. Indeed, as shown in the table 3 and 4 below, both price and quality (in terms of quality of customer service) are perceived by ECS users as two very important characteristics of the services, also in the switching decision.

Table 3 - Importance of (a) price and (b) customer service (2020).

And how important to you were each of the following?... Price (%)

	Very/ Fairly important	Not very/ Not at all important	Very important	Fairly important	Not very important	Not at all important
EU27 AVERAGE	90	10	51	39	7	3

And how important to you were each of the following?... The level of customer service offered by the provider (%)

	Very/ Fairly important	Not very/ Not at all important	Very important	Fairly important	Not very important	Not at all important
EU27 AVERAGE	88	10	50	38	8	3

Table 4 - Percentage and Reasons of switching (2020).

Have you switched your provider in the last year? Why? (%)

	Yes	The new provider is cheaper	The new provider offers a higher quality of service	I wanted different services that weren't offered by my old provider	I lost trust in my previous provider	For ethical reasons (for instance because I feel like the provider's conduct has a harmful impact on the environment or society)	I had to switch (for instance because I moved or because my old provider ceased to operate)
EU27 AVERAGE	12	44	30	6	10	2	7

[108] Recital 15 EECC.
[109] Ref. Manganelli A, Schnurr D (2024).

QoS can be distinguished into three broad categories: (i) customer-friendly/empowering contractual framework; (ii) customer care; and (ii) technical performance. We already dealt with (i) and partially (ii) in section 2.4.A.

As for (iii) **technical performance**, as mentioned, enhancing and differentiating technical QoS could be an important competitive tool, although quite uneasy to obtain because the information asymmetry between providers and end-users is usually high as far as quality is concerned, and anyway much higher than price information. Moreover, communications services are clearly 'experience goods' (one doesn't know or appreciate how much additional value a more reliable or faster connection or a better customer care/helpdesk provide until he has got it). This is also confirmed by the 2020 survey where 'previous experiences' was by far the most important reason when choosing a service. If 'previous experiences" was 'very/fairly important/ for 75% of people, 'recommendations from friends/family' was 53%, 'other reviews or comments online' was 33% and 'different forms of advertisement' was 19%.

It is important to point out that consumer information asymmetry is not only detrimental for consumer yet can also harm high-quality suppliers: if consumers fail to assess product and service quality and suppliers fail to communicate it, high quality products will be "displaced" by cheaper, lower quality products (according to the 'classical' adverse selection mechanism). Consequently, transactions that could be beneficial to both consumers and suppliers are not concluded, resulting in a welfare loss for the society. Thus, information asymmetry between consumer and supplier is not the basis (only) of fairness problems, but also, and more importantly, represents a traditional market failure. The typical solution to information asymmetry problems is proper disclosure (signalling) of those information consumers need to make informed choices.

Therefore, under this light, companies need to develop **effective informational mechanism of quality signalling**, which is of course much more difficult than price. Thus, again, independent, effective (possibly AI-empowered) quality assessment and quality comparison tools are even more important than mechanisms for price comparison.

Some tools already developed or overseen by regulators are: NRA survey based on NRA's measurements or appointed third party; NRA survey based on end-user experience (crowdsourcing); Speed test apps or online tools for end-users; Coverage map (with different speed) for end-users; Operators' quality rankings. According to a recent benchmark,[110] out of 14 EU countries scrutinised (i) 10 NRAs have developed speed test tools, both for fixed and mobile; (ii) 10 NRAs have built coverages Maps, both for fixed and mobile; (iii) 8 NRAs surveyed fixed QoS and 9 mobile QoS; (iv) 4 NRAs developed ranking of fixed operators and 5 of mobile operators. However, there are no clear data on the quality and effectiveness of such tools, which should be assessed, and which should be more and more be based on AI tools.

On the other side, given the asymmetric information and importance of signalling, rules must be in place in order to avoid unfair commercial practices and misleading advertising. At present the EECC contains few provisions regarding quality transparency.[111] However, those are quite legalistic

[110] Cullen International benchmark, February 2024, conducted on 14 counties (Belgium, Croatia, Czech Republic, France, Germany, Ireland, Italy, Netherlands, Poland, Portugal, Slovakia, Spain, Sweden, United Kingdom).
[111] Art 103 and 104.

consumer protection rules aiming to a minimum QoS to be respected[112] rather than aiming to build QoS as an observable variable on which providers can compete for end-users.

In this light, those rules should be **coordinated with (and probably absorbed by) those of the Open internet access regulation** (OIAR).[113] That said, the value added of both set of sector-specific rules about QoS transparency (within the EECC and the OIAR) should be assessed against an exclusive reliance on **horizontal rules**. All this would imply a radical shift from a regulatory-imposed QoS transparency to a commercially signalled QoS, i.e., again from consumer protection to consumer empowerment.

Finally, QoS as (iii) technical performance is of course (mainly) the result of innovative (long-term) investments and technological improvements. This means that regulators and policy makers should:

1. avoid a legalistic and consumeristic approach to demand-side policy that completely neglect and overlook existing **trade-offs between short term vs long term consumer interest**. In other words, when conceiving and implementing consumer policy, policy makers and regulators should be aware and weigh the existing trade-offs and the impact those could have on long-term consumer interest, related to investments and the improvement of technical performance (which could be more intense than those on the supply side).[114] This do not preclude, of course, policy maker to soften any of these market trade-offs for policies that they consider socially beneficial, by covering the cost via a Public Funding Model.

2. aim at reverting the increasing perception of communication services as homogeneous products and commodities[115] (which wouldn't require investments in innovative technologies), by also allowing companies to differentiate their quality retail offers and give the consumers the possibility to exercise their free and informed choices. Again, this would imply a shifting of the focus from price competition with a minimum QoS to quality competition. This possibility is often limited by rules that wants to paternalistic to protect users, while *de facto* excessively limiting their freedom to choose and the ability for companies to make the most out of their innovative investments. This is also clearly the case of net neutrality provisions (as described in the next section 3).

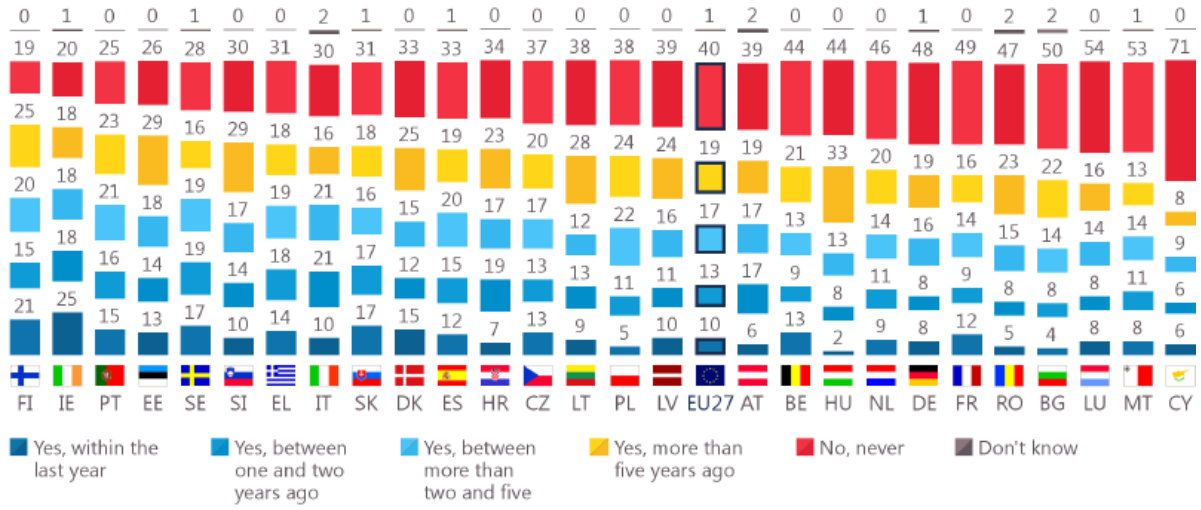
2.4.4. Switching, ease to switch and 'on-network' consumer empowerment

As mentioned, switching, and number portability provisions are aimed at removing obstacles for consumer to make informed and free choices, and should remain as sector-specific rules as far as related to development of competition by liberalising the demand side. Implementation of these empowerment strategies has reduced lock-in and switching costs and consequently **increased the consumers' propensity and tendency to switch operators**. According to the 2021 European

[112] i.e., article 103(2)(b).
[113] art 4(1) (d) & (e) OIAR.
[114] Indeed, regulatory trade-offs on the supply side, as referred to access regulation and access competition, has been extensively studied (i.e., productive efficiency vs allocative efficiency, and static efficiency vs dynamic efficiency). Much less attention has been devoted to the demand-side trade-offs.
[115] This is particularly true for consumer services, whereas business services could be much more differentiated and tailored.

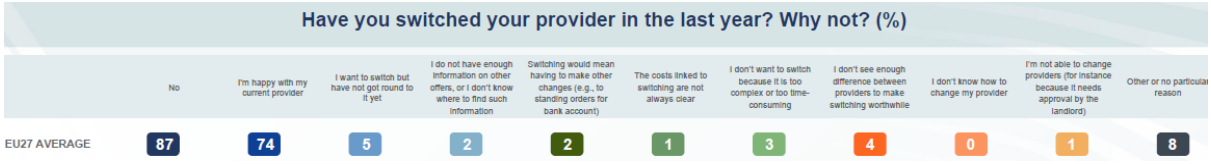
Commission's survey,[116] around 60 % of European consumers have changed telecommunications service provider at least once (table 5).[117]

Table 5: Switching provider (2021)



If one considers the legal monopoly as a starting point for the EC markets, this apparently unimpressive figure signals indeed a successful liberalisation and effective pro-competitive and pro-consumer regulation. In addition, in 2021, around 13% of EU consumers changed internet service provider in the previous 12 months. At a first look, also this figure is not impressive, since it does not signal very high churn rates. Nevertheless, it is very relevant that 74% of those 87% of users that didn't change provider said that their 'inertia' it was not really "inertia", rather a conscious choice not to switch due to the fact they were happy with the current service provider (table 6).[118]

Table 6: Percentage and reasons for not switching provider (2020)



Indeed, next to the actual switching and churn figures, it is even more crucial to assess the "ease to switch" provider, which represents a good indicator for the 'potential switching'. If on the supply side, market contestability and potential competition, i.e., absence of entry costs, are relevant as a

[116] European Commission (2021) E-Communication in the Single Market [Special Eurobarometer No. 510, June 2021].
[117] In 2017 that figure was less than 50%.
[118] European Commission (2020) market monitoring survey 2020 – internet provisions. The other reasons were "I want to switch but have not got round to it yet" (5%); "I don't see enough difference between providers to make switching worthwhile" (4%); "I don't want to switch because it is too complex or too time consuming" (3%); "I do not have enough information on other offers, or I don't know where to find such information" (2%); "Switching would mean having to make other changes (e.g., to standing orders for bank account)" (2%); "The costs linked to switching are not always clear" (1%); "I'm not able to change providers (for instance because it needs approval by the landlord)" (1%); "I don't know how to change my provider" (0%); "Other or no particular reason" (8%).

disciplining force, likewise, on the demand side, regulators and policy makers should focus on the ease to switch, and not (only) on actual switching numbers.

As a matter of fact, actual switching, and consequently market shares dynamics were obviously very important in the years after liberalisation, whereas, today, a regulated market with empowered consumers can find a competitive equilibrium with an asymmetric market share distribution among the different players and also one maintaining a prominent market position, because of its consumers have chosen not to switch (or to come back after having switched to (an)other provider(s)). In other words, consequently to liberalisation and pro-competitive regulation, market shares of the main EU operators have quite constantly declined, this decline does not need to necessarily be constant over time until the market is equally divided to prove a robust and enduring competition and consumer empowerment.

However, on the other side, market competition does not provide benefits for all consumers in the same way. If almost three fourths of inert consumers seem to undertake a conscious choice, however one fourth may not be engaging as in need of some form of further empowerment. Those could be somehow considered "**vulnerable" consumers** (who are not easy to be empowered).[119] Of course, also some part of the 75% of consumers could be affected by some behavioural biases and bounded rationality (e.g., an endowment effect).

On one side, this problem could be softened by the development of AI mechanisms guiding users toward the awareness of the importance of their choices and helping them in the selection of information, making the actual choice (including also not to switch), and the follow-up actions.[120]

On the other side, rephrasing and specifying the previous statement, low switching figures and asymmetric market shares are problems only if the positive impact of competition (downward pressure on prices and upward pressure on quality) can't reach the whole customer base. In other words, this becomes a problem if the positive effect of competition is not a *public good,* but it is *club good* (non-rivalrous but excludible) and the interaction between active/sophisticated users and companies does not exert positive spill overs effect on inert vulnerable users.

A revised regulatory framework could therefore consider the adoption of some **mechanisms aimed at somehow allow/nudge inert users to make a choice**. This shouldn't be a nudge/incentive given to consumers to switch provider, yet to empower them (allow and facilitate) to subscribe a better offer among those that the same provider gives to its sophisticated users (also those ones won-back from other providers). This would be an 'on-network' consumer empowerment, and its main challenge would be to calibrate that nudge in a way not to distort or influence satisfied consumers, but just "awake" the inert ones. Moreover, this could be also a way to balance the trade-off between productive efficiency and allocative efficiency: inert users are not forced or incentivised to necessarily switch, and larger companies to shrink, thus maintaining economy of scale, density, and scope yet tendentiously extending the positive effect of competition to all users.

[119] This concept of "vulnerability" is different from that developed as far as universal service is concerned. Those are not (necessarily) "low-income" users or users with "special needs". Indeed, bounded rationality is not a "special need", rather a characteristic which is, more or less present, in all individuals, yet over a certain threshold inhibit any form of empowerment.
[120] Fletcher, A. and Z. Vasas (2023).

These mechanisms could possibly soften price competition for the "active users" yet also avoid inert users (which often could correspond to certain categories, like the elders or uneducated) to cross subsidise them. Moreover, such mechanisms could also incentivise companies to focus more on quality competition rather than only on price. This would also avoid the regulatory-risk of potential new regulation introducing retail price caps, or compulsory stand-alone offers (see Ofcom 2017 statement[121]) which are based on 'universal service' rationales, yet in this case addressing a more general problem of vulnerability - not (necessarily) linked to "low-income" or "special needs" users (art 85 provision of affordable services)

In this direction some member states have introduced obligations for providers to **inform all customers, close to the termination of the contract and when making changes to the contract conditions, about the "best tariff"** available. The intensity of this requirement could be made somehow proportional to the duration of users' 'inertia' (considering here a strict concept of 'on-net' inertia). Thus, maybe, after a certain period of inertia at the same offer, also imposing an opt-in framework to the old offer (rather than on opt-out) and a related default change to the "best tariff". Best tariff is not necessarily an objective concept, as end-users surely have different preferences on different tariff configuration. Moreover, it would be much more effective to have information about a "best offer", including not only pricing parameters yet also qualitative aspects. That's where, again, support given by AI mechanisms and personalised comparison tools could be applied.

2.4.5. Addressing potential future lock-in and switching issues

As said consumer empowerment is interlinked with competition enhancement, therefore **switching and lock-in issues on the demand side are correlated to supply-side market configuration and regulation**.

It will be important to investigate specific switching and lock-in dynamics for services on the FTTH, which may be different from those on the FTTC/DSL networks, as access remedies may be different. For example, evidence to date seems to be showing much lower switching rates on FTTH than on copper. This is possibly related with material switching costs for FTTH connections of installing a new line into a house. This depends very much in a co-evolutive manner, on one side, on the market structure (e.g., if there will be more than one operator vertically integrated) and, on the other side, on the kind of supply-side regulation (e.g., moving away – to a certain extent – from access regulation/resale). Therefore, depending on the changes on supply side, measures to reduce the installation costs would be crucial, as well as to increase 'on-network empowerment'.

As far as mobile markets are concerned, there are no such generalised installation costs and switching problems. Nevertheless, an important issue that consumers may face in the future is possible lock-in

[121] Ofcom (2017) Review of the market for standalone landline telephone services, which found that voice-only customers were receiving poor value for money compared to customers who had bundles of landline, broadband and/or pay-tv services and thus proposed to regulate BT retail prices. Since April 2018, the prices these customers pay for their voice-only service have been protected by BT's voluntary commitments. These commitments have been renewed by BT (and accepted by Ofcom) to ensure continued protections for voice-only customers until March 2026. This was particularly important to older customers, since nearly two thirds of customers who only had a landline were over the ages of 65, and more than three quarters had never switched provider. Consequently, a class action lawsuit has begun in January 2024, seeking compensation over claims the telecoms group allegedly overcharged for landline services.

phenomena regarding consumers' IoT devices such as cars, smart home equipment etc. Thus, the forthcoming regulatory framework, considering an ecosystemic approach, should cover also issue related to unbundling of connectivity from devices and effective switching procedures. A possible solution, that market is starting to autonomously develop, is the diffusion of e-SIM,[122] which would reduce lock-in risks, as for M2M use-cases, and would make it easier to switch and reduce switching costs (also for providers) for the human/consumers markets. The EECC currently requires NRAs to promote "over-the-air" (OTA) provisioning– i.e. fully digitised processes,[123] which of course would be supported by e-sim. However not so much has been done in that direction, and, of course, the diffusion of e-sim has network effects - which could worsen rather than softening lock-in issues if that technology is not widespread.

Some possible strengthening could be done under art 106.6, which enables NRAs to establish the details of the switching and porting processes and requires that could be including, where technically feasible, a requirement for the porting to be completed through over-the-air provisioning, unless an end-user requests otherwise. [124]

Finally, in an extended value chain environment, the **switching provisions should be coordinated with existing legislation** that separately and specifically deal with that regulatory issue for specific markets and segments. First, the Data Act that disciplines quite extensively and in depth the switching process for the Cloud markets,[125] and secondly, few provisions of the Digital Markets Act, for example art 6.6, regarding switching and multi-homing restrictions, and art 6.9 regarding data portability, for gatekeepers in the core platform services.

[122] An eSIM is a form of programmable SIM and contains the same information as a traditional SIM card about a customer's identity and connection to a mobile network. Whereas provisioning traditional SIMs involves the physical insertion or swap-out of the SIM card, eSIM together with 'over-the-air' (OTA) technologies make it possible for the mobile subscriber to provision and change their subscription and operator remotely. Furthermore, each eSIM has the potential to contain multiple different user profiles.
[123] EECC, Article 93.6.
[124] See Wik (2021).
[125] See Manganelli A, Schnurr D (2024).

3. From Net Neutrality to Ne[x]t Neutrality

3.1 Rationale(s) of the Net Neutrality debate(s)

In the previous section 2, we mentioned the issue of a level playing field between telecom companies and digital platforms providing substitute services (i.e., NIICS) with regards obligations imposed by demand-side regulation.[126] Nevertheless, **traditionally digital platforms (as those providing NIICS) as well as other 'content and applications providers' (CAPs) have mainly complementary relationships with Telcos**. As a matter of fact, this was the exclusive type of relationship before the internet ecosystem started to be more concentrated and centralised and the traditional boundaries between the various actors started to be increasingly blurred. As for the complementarity relationship, on one side, telcos enable the distribution of content and services to end-users, by deploying (high-speed) telecommunications infrastructures and providing end-users with internet access services. On the other side, an end-user needs and buy both a broadband connection and online contents and applications.

In the original internet landscape, characterised by a situation where internet usage mainly involved simple email exchanges and web browsing, with a quite decentralised and symmetric data flow, needing low bandwidth, there were an **asymmetry in the complementarity** relationship between Internet Service Providers (ISPs or IAS providers) and CAPs and that was one of technical nature. Indeed, ISPs have the material and technical capacity to manage data traffic (i.e., *throttling*, prioritising or blocking), consequently, affecting the service quality (or even the availability for end-users) of content and application, whereas the opposite was not possible. Moreover, under an economic perspective, depending on their scale and the competitive environment, ISPs can be (competitive) bottlenecks for CAPs to access end-users and, thus, in a situation where CAPs had no countervailing power, ISPs could exert market power, by applying non-price discrimination practices on CAPs' services. Indeed, in a situation of decentralised, symmetric traffic flaw needing low bandwidth, with very scarce risk of congestion, traffic management and differentiation could be hardly justifiable as aimed to an efficient use of the network resources.

In this context, the *network neutrality* debate original concept was expressed as "*all data packets on the Internet should be treated equally*",[127] therefore framing the internet traffic on an inherent "best effort" approach (which was completely appropriated for non-time-sensitive applications). Afterwards, the net neutrality concept(s) and debate(s) took on many different hues and forms depending on the market and policy context. Its consolidated basic definition still concerns: (a) the prohibition of payments from content providers to internet service providers aimed to favour their own contents; and (b) the prohibition of traffic prioritisation (*fast lane* versus *dirty roads* or *managed services* versus *best effort*), with or without compensation[128] (with some exceptions for specialized/managed services like broadcast)

[126] Similar considerations can be raised about asymmetric and unbalanced regulatory pressure on the supply-side regulation, especially before the enactment of Digital Markets Act (DMA) and Digital Service Act (DSA).
[127] Wu T (2003).
[128] Greenstein S, Peitz M, Valletti T (2017).

The underlying theoretical assumption was that, without any net neutrality obligations, ISPs would set a system of data paid termination, as for voice calls. **Anti-competitive concerns** would arise that an ISP would charge high and/or differentiated termination fees, combined with non-price discriminations, to reduce competition (by blocking CAPs or degrading their QoS) and exclude competing content providers, if an ISP is vertically integrated and provide content or application services, or, anyway, exploit CAPs.[129]

Indeed, in the US (where the NN debate originated), the risk of self-preferencing by vertically integrated ISPs, with anticompetitive exclusionary effects on other CAPs, was and is one of the main concerns as for the neutrality of the internet. In the US dominant ISPs are vertically integrated (e.g. Comcast – which merged with NBC-Universal in 2011 and with Sky in 2018, and AT&T -which merged with Time Warner in 2018) and thus offer in bundles communications and audio-visual managed services, directly competing with global digital platforms (hyperscalers) and other CAPs. [130] In some EU member states, triple and quadruple-play bundles including digital television started to become widespread. However, in the EU there is not such a widespread vertical integration between internet access providers and audio-visual content as there is in the US. [131] In addition, differently from the EU, US Internet access market is concentrated end-to-end and competitive pressure is quite limited.

Further to the discrimination and market power rationale, another important and different aspect of the NN debate was related to the **internet traditions of freedom, openness, and equality**. Indeed, the internet was born and developed under a kind of natural net neutrality regime, not imposed by regulation but resulting as a spontaneous market outcome from decentralised market interactions. In the EU, the net neutrality debate has been mainly developed under this conceptual framework, as an end-user's right to access digital services and contents in a universal, equal, and non-discriminatory manner.[132] This is why the EU Open Internet Regulation (2015), [133] did not actually modify the access and interconnection regulatory regime, dealing with market power and anticompetitive discriminations, but those rules regarding universal services and users' rights.

As briefly described, NN rules (depending on their configuration) have impacts on different aspects and sides of the digital ecosystem. On one side, there is the end-users' ability to freely access and distribute information, content, and services; on the other side, there are the economic relationships between ISPs and CAPs and how this could impact consumer welfare and how, in turns, competition dynamics (in the two sides) could impact the relationship between ISPs and CAPs. As we will see in the following, the EU net neutrality regime seems to mainly refer to the first aspect, surely considering

[129] Should it be the case, it was also suggested to define data transmission and termination as relevant markets with a SMP identification and cost-oriented prices as a remedy: see Larouche P (2012). Indeed, a direct restraint on ISP market power, taking into account the two-sides of the access market, would represent a less distortive solution and be more consistent with the overall regulatory framework than any net neutrality measure. For example, Net Neutrality as a zero-pricing rule can be considered a constraint on the business model of the ISP, as two-sided platform (intermediating CAPs with end-users), forcing it to adopt a one-sided business model (i.e. charging only users and not CAPs.)

[130] Cave M, Vogelsang I (2015).

[131] The closest case in the EU was the conditioned clearing decision about the Liberty Global/Ziggo merger, for concerns about degrading rival broadcast channels.

[132] Nevertheless, differently from the universal service obligations concerning electronic communication services, the universality and non-discriminatory provision of digital contents was not based onto regulatory obligations for the providers of those services, but for the network intermediaries. In other words, NN rules in EU have been designed as Universal service obligations imposed to telcos in order to allow universal access to contents and therefore the possibility for users to buy contents and applications and for CAPs to sell their products/services.

[133] Regulation (EU) 2015/2120 laying down measures concerning open internet access.

also some technical and efficiency needs for traffic management, yet considering less the economic relationships between ISPs and CAPs, and consequently their evolutions and changes and the impact that this may have in the overall digital ecosystem.

3.2 Current EU Regulatory Approach

The EU Open Internet Regulation grants end-users with enforceable rights to access and distribute information, contents, and services. [134] Consistently with the EECC, the 'end-users' concept within the OIAR includes businesses inasmuch as they rely on an IAS to reach their customers.[135]

In doing so, this place obligations on ISPs to "**treat all traffic equally** ... without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used."[136] However, "reasonable" day-to-day traffic management practices are allowed as long as they are (a) transparent, (b) non-discriminatory, (c) proportionate, and (d) not based on any commercial considerations but on objectively different technical quality of service requirements for specific traffic categories. In any case, these measures may be maintained no longer than is necessary and cannot involve deep packet inspection. Some practices are clearly considered non-reasonable that "block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services ".

There are three general exceptions to the rule where compliance with legal obligations, network integrity and congestion management in exceptional and temporary situations are involved.

Regulation also allows for the provision of *specialised services*, deemed as those services "optimised for specific content, applications or services … where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality"[137] or, in other words, those services that need to be carried out at a specific level of quality that cannot be assured by the standard *best effort* delivery. The regulation defines specific safeguards to be respected for the provision of specialised services to ensure that the open Internet is not negatively affected. Specialised services (a) can be satisfied by the network capacity residual to any IAS provided; (b) are not usable or offered as a replacement for internet access services; and (c) are not to the detriment of the availability or general quality of the internet access for end-users.

Furthermore, the regulation defines **transparency obligations** for providers of internet access services additional to those existing for electronic communication service providers.[138] In particular, contracts for internet access services must include easily accessible, accurate, meaningful and comparable information, covering (a) any traffic management measures used, and any impact on the end-user (e.g., quality of internet access, end-user privacy and personal data protection); (b) any data caps, speed and other quality of service parameters which may in practice impact internet access; (c) how any specialised services, to which the end-user subscribes, might in practice affect the same end-user's

[134] Art 3(1) OIAR - Safeguarding of open internet access.
[135] This is clearly stated in art 2 OIAR, which generally refers to EECC definitions, and then clarified by case law: joined Cases C-807/18 and C-39/19, Telenor Magyarország Zrt., para 36- 39.
[136] Art 3(3) OIAR.
[137] Art 3(5) OIAR.
[138] Art. 4 OIAR.

internet access services; (d) the download and upload speed of internet access services (with different metrics depending on fixed or mobile network); and (e) the remedies available to the consumer in case of any regular discrepancy between the actual performance of the internet access service and the contractually agreed on one.

As for enforcement, **national regulators are empowered to closely monitor** market developments and assess traffic management, commercial agreements and the compliance with transparency obligations in order to ensure the availability of non-discriminatory and transparent internet access at levels of quality that reflect advances in technology. For this purpose, national regulators may impose minimum quality of service requirements on internet access providers and other appropriate measures to ensure that all end-users enjoy an open internet access service. They must report annually on their findings to the Commission and the BEREC.[139] Moreover, according to the regulation provisions, in order to enhance a consistent application of the regulation, BEREC drew up detailed guidelines, in 2016, 2020 and 2022, which national regulators must take strictly into account. [140]

Zero-rating Practices

EU NN regulation explicitly established the freedom to conclude agreements between ISPs and end-users relating to commercial and technical conditions, as well as IAS aspects regarding price, data volumes or speed, and any commercial practices. Nevertheless, such agreements and commercial practices must not represent a limitation in the exercising of end-user rights and, consequently, circumvent provisions safeguarding open internet access.[141] In this context, one of the main points of debate about net neutrality concerned the *zero-rating*, which is a commercial practice whereby an ISP does not subtract data usage associated with specific content or a class of content from a customer's data allowance.

Initially this practice has been considered compatible, on a case-by-case basis, with net neutrality regulation (2016 and 2020 BEREC net neutrality guidelines). Under those BEREC guidelines only some practices were clearly prohibited – for example, those where all applications are blocked or slowed down once the data cap is reached, except for the zero-rated application(s). Other practices were considered in need of a specific operational assessment to be carried out by NRAs using the following criteria: (a) whether the practices circumvent the general aims of the regulation (to "safeguard equal and non-discriminatory treatment of traffic" and to "guarantee the continued functioning of the internet ecosystem as an engine of innovation"); (b) the market positions of the ISPs and CAPs involved; (c) any distorting effects on end-user choice, both for applications and CAPs; and d) the scale of the practice and the existence of alternatives.

In September 2021, the Court of Justice of the European Union (**CJEU) issued three rulings that found zero-rating offers to be unavoidably in breach** of the requirement of equal treatment of traffic in Article 3(3). Subsequently, in June 2022, BEREC revised its Guidelines to reflect these rulings.

[139] Under art. 5 OIAR, NRAs have published so far three set of yearly report, which have been sent to the Commission and BEREC.
[140] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, BoR (16) 127, and afterwards BoR (20) 112, and lately BoR (22) 81.
[141] Recital 7 and art 3(2) OIAR.

Zero-rating practices are based on *data cap usage commercial practices*. The latter are not covered by net neutrality rules and are normally allowed as retail markets are not regulated. A data cap is a legitimate pricing strategy as well as a measure to somehow avoid congestion, yet also create an artificial scarcity, making different content work as substitutes for end-users and, thus, intensifying the competition among content providers.[142] As for the general case, in this context of *data cap commercial offers,* zero-rating represents a contingent competitive concern where a vertically integrated ISP would exempt its own traffic, in order to favour its content. A connected yet different issue is that of *zero-rating* agreements with a third-party CAP. In this situation, data caps could induce CAPs to compete for the "fast/zero-rated lane". In this competition, larger CAPs would likely to prevail, also because of their must-have contents, usually in exchange of prioritisation or data-free payment. So, by prohibiting zero-rating, policy makers want to avoid large CAPs locking-in users. Yet again an obligation aimed to impede large CAPs exertion of market power is however imposed on telcos.

3.3 What to Look Into

3.3.1. Are there technological and/or market changes no longer matching OIAR assumptions?

A first issue to investigate is whether an internet ecosystem composed of decentralised and atomistic users that symmetrically exchange traffic, information and content does still exist. Nowadays, this vision of the web as a place where individuals and small enterprises interact in a decentralised way is no longer true due to the transformations the internet and the web have undergone, both in terms of structure – centralised versus decentralised – and data traffic – symmetric versus asymmetric.

Today, the **great majority of internet data packets** are related to contents and services which are mostly unidirectional - from content providers to users - and use high bandwidth and a quality of service that decreases drastically with delays.[143]

In addition, digital content markets and services are concentrated, and few large CAPs (Very large Online Platforms/Gatekeepers) have significant market power and provide "must-have" contents and applications to end-users and business-users. In such a situation, notwithstanding their 'termination bottleneck', there is a question whether **ISPs can 'behave independently'** of its competitors and customers' and exploit market power, regardless any net neutrality regulation. Indeed, due to the competition between ISPs for end-users, due to decades of pro-competitive access regulation, any activity by ISPs blocking or degrading the quality of those must-have contents/applications to their subscribers, could be 'sanctioned' by (empowered) end-users by switching to another ISP.[144] These changes had a direct impact on the assumption that no CAPs have countervailing power vis à vis ISPs

[142] Economides N, Hermalin E (2015).

[143] This is a general statement that is overall true, yet based on a simplification of the dynamic within the internet ecosystem as there are large difference between CAPs. Those differences are based on the size, yet also on the type of content/application provided. For example, traffic from cloud services is largely balanced and mostly happens off-peak. For detailed general reference, see Analysys Mason (2022), p.23; TeleGeography (2023), p. 7. Ericsson (2022) Mobility Report, p. 18; Sandvine (2023), p. 22. Arthur D. Little (2023), p. 18.

[144] Cave M, Vogelsang I (2015). Regarding any possible coordination in this respect there are competition law instruments in place.

and therefore on the assumption that ISPs may have positive economic incentives to discriminate or to exploit market power for economic reasons.[145] Indeed, large CAPs have been increasingly investing in their own infrastructure such as backbone networks (e.g. submarine cables), CDNs, data centres, hosting and cloud computing.[146]

Therefore, another issue to assess, is whether is still true that only ISPs can influence the traffic. In this regard, an open question originating from the technological development in mobile 5G communications concerns whether other subjects than network operators, e.g., operating system, could somehow control the network slices.[147] Another evolutive scenario is that APIs developers may be able to programme the virtualised network to support new applications, rather than relying upon telcos to introduce new capabilities themselves. An example is that developers might programme the network to favour some types of traffic over others. Therefore, **ISPs may not be the only ones who control how traffic is managed on the 'network'**, as the current NN rationales and regimes assume.

More generally, **ISPs seems to be no longer the sole players capable to influence the end-users' internet experience**, being now growing significance in what other players in the extended value chain can do.

For example, as for investments in transport infrastructures, large CAPs reduce their dependency on "traditional" backbone transit providers, which can be bypassed. Consequently, large CAPs increasingly interconnect directly with IAS providers: such direct peering may also help to improve performance while at the same time providing large CAPs greater control over that performance and the routing path. [148]

Furthermore, Content Delivery Networks (CDNs)[149], deployed by third parties (commercial CDNs) or increasingly by large CAPS (private CDN), which typically place their cache servers in the ISPs' access networks (on-net CDNs), enable to some extent service differentiation by managing traffic via private networks and ensure content is hosted as close to the end-user as possible to guarantee certain quality levels.[150]

CDNs, namely on-net CDNs, represent a very positive development for the network services since they (i) allow to bring traffic closer to the end-user thus minimising the traffic load, and (ii) reduce cooperatively capacity costs for ISPs. Notwithstanding, from a user experience perspective, these and other mechanisms can act as 'technological substitutes' for network management by ISPs, ensuring high quality of experience perceived by the end-user[151] which should be taken into account by regulation. Indeed, the fact that large CAPs 'buy' services from a commercial CDN or 'make' that

[145] Of course, smaller CAPs have a relative disadvantage compared to large CAPs when bargaining with IAS providers: a) smaller CAPs would face (relatively) higher transaction costs, b) they may less likely avail of "must have" content and c) it may be more difficult for a smaller CAP to enter into a commercial partnership on its services. BEREC Draft Report on the IP Interconnection ecosystem – BoR (24) 93.
[146] BEREC Draft Report on the entry of large content and application providers into the markets for electronic communications networks and services - BoR (24) 51.
[147] *Ibidem*, Bor (24) 51.
[148] BEREC Draft Report on the IP Interconnection ecosystem – BoR (24) 93.
[149] Article 6 (32) of the Directive EU 2022/2555 (NIS2) defines CDN as a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers.
[150] Stocker, V., Smaragdakis, G., Lehr, W.H. & Bauer, S. (2017).
[151] Briglauer W (2024).

service, by vertically integrating, can be seen under an economic perspective as a form of 'paid prioritization' although traffic is not prioritized in the network layer, and thus it is not subject to OIAR.[152]

3.3.2. Is there (still) need for NN rules? What kind?

In a context of crucial technological and market evolutions, a primary reflection should be devoted to whether net neutrality rules are still needed or whether there is room for an efficient radical reform of the principles underlying the current OIAR.

In addition to more recent changes, many of the economic effects of Net Neutrality rules have never been fully considered, *ab origine*, by the current EU legislation. Indeed, the OIAR looked at NN as a policy almost exclusively concerning protection of end-users' rights, which of course is a paramount objective, yet not the sole one.

Indeed, due to this defect, some economic analysis really questioned at the basis the positive impact of NN rules. In this regard, some economic literature has focused on the question of whether a competitive IAS market could make net neutrality rules (e.g., prohibition of payment against a "fast lane") redundant in terms of preventing anti-competitive behaviour. Recent theories have generally supported the idea that lifting net neutrality rules on competing platforms is welfare-increasing.[153] Competition may influence the desirability of net neutrality provision concerning investments in broadband capacity and content innovation. In allowing a payment fast lane, both would increase compared to a net neutrality regime.[154] Empirical contributions are few, yet a very recent literature review shows that **net neutrality regulations have negative impacts on high-speed network investment** by (wireline) ISPs, which is in line with most theoretical contribution, and, in the long term, is likely to imply negative welfare effects. [155]

Nevertheless, a balanced assessment must not fall in the opposite extreme and overlook some of the core objectives NN rules, i.e., maintaining an open internet and protecting consumer freedom of choice for contents. For example, particular attention should be given to safeguarding audio-visual media services of general interest.[156] Indeed, "protecting and promoting a neutral and open Internet where content, services, and applications are not unjustifiably blocked or degraded" [157] should remain an overarching objective for the Digital Decade. So, the main point is to aim for rules which allow to achieve these objectives, by minimising the distortive impact on economic and market dynamics. In

[152] Garrett, T., Setenareski, L. E., Peres, L. M., Bona, L. C. E. & Duarte, E. P. (2022).

[153]This outcome is due to the intense competition among ISPs resulting in better prices for end-users and lower overall price distortions and not to competition reducing the incentives of ISPs to discriminate between content providers, as in the voice call termination (where the 'real' market failure is one related to network externalities and not one of market power), see also Cambini C., Valletti T. (2005).

[154] Bourreau M, Kourandi F, Valletti T (2015).

[155] Briglauer, W., Gugler, K., Cambini, C. & Stocker, V. (2022); Briglauer (2024).

[156] As for the prominence principle foreseen under art 7a of the AVMSD and recital 29 of Directive 2018/1808/EU. This is because of essential role that AVMS of general interest play in driving media pluralism, freedom of speech and cultural diversity. That special status is very often associated, at national level, with further obligations (such as the provision of newscasts) to better pursue those values and general interest objectives.

[157] EU Parliament, Council and Commission (2023) European Declaration on Digital Rights and Principles for the Digital Decade.

other words, NN rules should embrace a general principle of the EU law: the "**proportionality principle**", which is also a well-recognised for the supply side access regulation in the sector.[158]

On the contrary, the **OIAR and its interpretation clearly moved away from that approach by adopting a "precautionary principle"**, thus imposing a strong restriction on regulated entities in view of a maximum probability of effectiveness. However, this approach inevitably leads to the risk of increased costs for the regulated company, inefficiencies in the market and social costs.

A balanced and future-proof call for a neutral network should involve a proportional, dynamic, and systemic response to issues originating from digitalisation, multimedia convergence, network virtualisation and the overall modular structure of the current digital ecosystem.

Here, the idea of **'ne[x]t neutrality', that is to define rules aimed to cover all contexts of opacity and non-discrimination in each of the relationships constituting the digital transaction, by assessing substitutability and complementarity of services and preventing or counteracting exertions of power across the whole digital extended value chain**, thus considering all the network and ecosystemic effects. Indeed, each digital transaction in the digital ecosystem is multifaceted and entails an array of interdependent bilateral relationships, namely: (i) end-user to end-user; (ii) end-user to ISP; (iii) End-user to CAP; and (iv) ISP to CAP.[159] Non-discrimination and transparency principles should be applied to each of the above relationships, reflecting a different side of net neutrality. If regulation focus only on one specific side, by imposing strict rule, and do not focus on others (or develops rules in an uncoordinated way) it neglects existing interdependences and trade-offs or, worse, unintentionally generate or enhance contractual or market power situations elsewhere.

Ne[x]t neutrality rules and their implementation should therefore be much closer to market analysis and pro-competitive regulation, including the key role played in the market by empowered consumers and end-users. [160] An end-user-empowering approach to net neutrality could be the best way to guarantee a freedom of choice, by allowing the end-users to decide what kind of internet access they would prefer, without over restricting the economic and commercial freedom of companies. As the current rules stands, ISPs are restricted to offering only basic packages of service, that ultimately lead, in some circumstances, to limit rather than enhancing consumer choice, and to have some customers subsidising others (e.g., normal vs heavy users). Whereas an enhanced flexibility for operators would give them incentives to innovate and create more bespoke and dynamic services, thus benefiting consumers' choice and welfare and also helping to address their investment needs (as explained in the next section 4).

[158] The proportionality principle is a general EU law principle, especially when it comes to economic regulation. Under Article 5(4) TEU, it applies at macro level for the definition of the scope of regulation (in the law-making process), yet this principle always applies at micro level as well, in the enforcement activity, for instance for the access regulation in the EECC, e.g., art 68.2 "In accordance with the principle of proportionality, a national regulatory authority shall choose the least intrusive way of addressing the problems identified in the market analysis."

[159]Being the last one (iv), in turns, itself multifaceted and complex, involving (i) substitutability; (ii) cooperation and (ii) complementarity relationships BoR (24) 51.

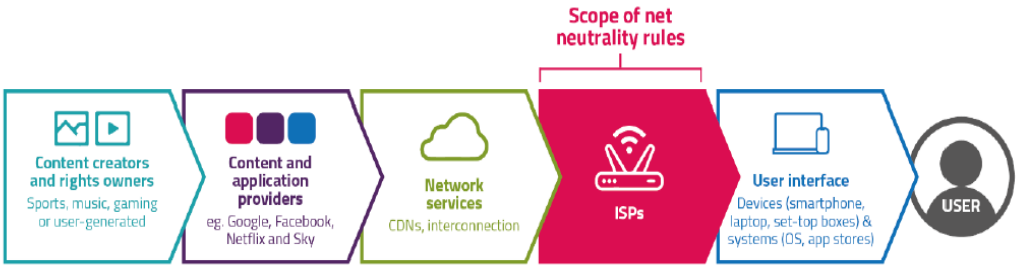
[160] Manganelli A, Nicita A (2020).

3.3.3. What are the asymmetries and distortion in the current approach?

The **current rules have no systemic approach for NN policy and target only one part of the extended value chain. This approach creates a regulatory fragmentation which may be unfit for the current converged ecosystem**. This fragmentation can be also explained with the existing (yet evolving) regulatory distinction of services: (i) electronic communications, (ii) audio-visual media, and (iii) information society services, which is now proving progressively inadequate as it frames competing (or anyway interplaying) services into different regulatory regimes.

Within the current EU approach (table 7), "net neutrality rules limit the actions ISPs can take, but do not restrict other parties in the value chain. Since the rules were put in place, players with strong market positions have developed throughout the internet value chain and are not constrained in the same way as ISPs by the net neutrality rules."[161]

Table 7: Digital ecosystem and scope of NN rules



Source: Ofcom diagram

Indeed, thinking "out of the (regulatory) box", if one frames these concepts and dynamics, transferring telcos' intermediary function into the digital platforms' intermediation shows again the asymmetric treatment: digital platforms, for example search engines or social networks, can, *mutatis mutandis*, prioritise contents that pay for a "fast lane", i.e., sponsored contents (and that possibility is not affect by the newly adopted regulation which focus only on the transparency and users awareness of these practices); whereas the same possibility is today not allowed at all to ISPs, even if end-users themselves request it.

Furthermore, telecommunications operators have been subject for more than two decades to pro-competitive access regulation on the supply side,[162] which has increase competition on fixed and mobile IAS markets, whereas a less restrictive approach was undertaken (especially before the enactment of DMA and DSA) for very large digital platforms.[163] The combination of these two elements implies that, on one side, **ISPs may have less economic incentives than in the past to manage traffic**

[161] Ofcom (2023) Statement – Network Neutrality Review.
[162] Along with a strict enforcement of merger regulation. Impeding any consolidation.
[163] Despite the 2018 adjustments of the scope of the ECCC, digital services and "traditional" communication services are based on an uneven playing field: the electronic communications pro-competitive regulation has created highly competitive telecoms markets (also by blocking consolidation through a strict enforcement of merger regulation). The recent approval of Digital Markets Act (DMA) and Digital Service Act (DSA) has introduced a more stringent set of rules for very large online platforms (as defined by DSA) and gatekeepers (as defined by the DMA), however neither of these new regulatory regimes really tackles the significant concentration of market power.

to deteriorate the end-users' experience and restrict their choice; while, on the other side, may have created an asymmetric negotiation and bargaining power between telcos and the largest CAPs.

To be sure, an asymmetric bargaining power do not represent *per se* a market failure and, in principle, do not require any regulatory intervention. However, the point here is not having an additional regulatory intervention, rather modifying the existing one. As a matter of fact, what could be seen as a market failure is the 'market incompleteness', mainly caused by the current regulatory approach, which does not allow certain market transactions between ISPs and CAPs to take place (transactions that may well have been efficient and welfare enhancing). Therefore, a possible intervention should be aimed to correct a possible existing "regulatory failure". Indeed, these impediments are not only depending on market and bargaining powers asymmetry but are also based on legal provisions, since net neutrality prohibitions have augmented the existing asymmetry.

Here, another important asymmetry in the NN approach can be described when there are dominant CAPs with must-have contents: **NN prohibitions are one-way directional**, i.e., put obligations upon ISPs not to discriminate among CAPs traffic, whereas there are, in principle, no limitations for CAPs should they want to discriminate among ISPs.[164] Although it could be assumed that CAPs have no incentives for discrimination, at the moment, this is a perspective scenario that a future-proof systemic regulatory approach should take into consideration, especially in a situation of (i) extension of the value chain, (ii) entry and vertical integration of large CAPs into the markets for electronic communications and (iii) progressive transformation of interactions between CAPs and ISPs in this extended ecosystem, from complements to substitutes[165] (allowing them to play a significant role in shaping the end-user experience).

One of the first "extension" of CAPs within the traditional value chain was **related to VOIP services**, which was one (or the only) economic triggers in EU for development of Net Neutrality rules in order to avoid the possible throttling/blocking practices by telcos of interpersonal communications VOIP services. IP interpersonal communication services and IAS are in a vertical relationship and upstream discriminations could have been aimed to favour Telcos' own interpersonal communication services.

However, the paramount difference is that in this case the possible discrimination rationale is not based on the provision of contents and applications by telcos, but on the fact that a content/application 'became' an electronic communication service, as recognised later on by the current regulatory framework, defining the concept of Number-independent Interpersonal Communication Services (NIICS). This approach allowed CAPs to enter the ECS market and offer competing ECS services, being subject to (generally) a lighter regulatory regime, whilst being protected under the OAIR, as complementary services.

So, even considering the current regulatory differentiation between access and interconnection,[166] under an economic perspective, it is unclear why an extension of the value chain should imply such a

[164] As a matter fact, possibly, art 6(6) of the Digital Markets Act (DMA) would limit CAPs' discrimination vis à vis ISPs,[164] but only if those "contents and applications" can be qualified as one of the core platform services and those companies are qualified as gatekeepers.

[165] See, BEREC Draft Report on the entry of large content and application providers into the markets for electronic communications networks and services - BoR (24) 51.

[166] In this regard, it is worthwhile highlighting that the EECC differentiates between access, defined as "*making available of facilities or services to another undertaking … for the purpose of providing electronic communications services, including when they are used for the delivery of information society services or broadcast content services*" - EECC art 2(27), and

substantial regulatory asymmetry, especially if we are dealing with substitute electronic communications services. **The asymmetry here is even more evident** if one considers that, likewise CAPs and ISPs, under an economic perspective, **all types of different upstream and downstream electronic communications services are always in a complementarity relationship (**also those provided by an access-seeker and an access services provider).

This seems to represent a weakness of the current regulatory framework, deriving from the mere juxtaposition of uncoordinated pieces of legislation - that should be instead seen and framed now as a part of a convergent extended framework for the digital ecosystem.

3.3.4. Do the current rules inhibit telecom industry to fully deploy new technologies capabilities?

The main consequences of (i) not looking in depth at the economic impact of NN rules; (ii) having an asymmetric approach vis à vis the different actors in the digital ecosystem and (iii) adopting rules inspired to a "precautionary principle" may be related to negative impacts on the currently regulated entities, both under an economic and financial viewpoint and in terms of their ability to invest and innovate. As for the latter, we refer mainly to the progressive deployment of 5G mobile networks, bringing increased opportunities to provide different services with different quality of service (QoS) levels in an unprecedented way.

Therefore, an additional assessment to do is whether and how the current rules can be interpreted and applied in a way that **allow telcos enough market freedom and flexibility (like it has always been allowed in the other, very innovative, segments in the digital ecosystem), or they prevent this new functionality being deployed and monetised properly**. 5G innovation is strictly interlinked with applications and use cases that differ significantly in their network requirements (which is clearly in contrast to the best-effort approach underlying the original net neutrality debate). 5G mobile broadband is mostly about QoS and QoE differentiation: therefore, if regulators and policy makers want to promote 5G deployment and developments of innovative 5G use-cases, they should also start from the assumption that QoS and QoE differentiation are efficient practices and should be allowed and encouraged as much as possible. [167]

As highlighted by the EU commission in its recent report on net neutrality "the regulation was deliberately conceived as a principle-based set of rules that could be applied to the foreseeable

interconnection, defined as "*a specific type of access implemented between public network operators by means of the physical and logical linking of public electronic communications networks used by the same or a different undertaking in order to allow the users of one undertaking to communicate with users of the same or another undertaking, or to access services provided by another undertaking where such services are provided by the parties involved or other parties who have access to the network*" – EECC art 2(28).
Those definitions imply that, on one side, 'access' is a very broad concept, and, on the other side, 'interconnection' is a specific type of access. Therefore, the differentiation between 'access' as one-way phenomenon and 'interconnection' as two-way phenomenon is based on economic rationale (i.e., who is providing a valuable service to whom) and not on traffic flows. In other words, 'access' is one-way under an economic conceptualisation, while there are always two-way traffic flows at the point of access. As a mere example, if there is a LLU disaggregation, the access-seekers and the access service providers exchange traffic and data in both directions at the local exchange point (regardless of possible interconnection of the different end-users belonging to different networks).

[167] Yoo C (2023).

development of new technologies" [168] This is true, yet on one side principle-based rules could bring legal uncertainty (which could inhibit innovations), and, on the other side, also principle-based rules could be over-restricting, i.e., excluding too many possible market transactions from the set of licit behaviours. [169] In order to reduce ex-ante uncertainty, BEREC has provided guidelines, yet those guidelines cannot modify the structural precautionary approach of the regulation.[170] In this regard, the EU commission has recently issued a report on the implementation of the current rules, signalling that: "*Greater legal certainty could therefore be beneficial to both innovators and consumers in the future*".[171]

Another assessment, with a wider and unconstrained perspective, has been done by **the UK regulator Ofcom, which is reconsidering the overall net neutrality regime** in order to clarify the applicable rules and relax some constraints for ISP activity: the current rules "*may be restricting their ability to innovate, develop new services and manage their networks. This could lead to poor consumer outcomes, including higher costs, or consumers not benefiting from new services as quickly as they should, or at all. These potential downsides might become more pronounced in the future, as people's use of online services expands, traffic increases, and more demands are placed on networks*."[172]

As mentioned, the rules currently in force allow for ISPs and CAPs to offer 'specialised services', that are "*services other than IAS which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality*". [173] This seems to be the crucial point. To be compliant with the Regulation, 'specialised services' are required to meet a range of criteria: (i) they should be services other than IAS services (and therefore cannot be usable or offered as a replacement for IAS); (ii) they are optimised for specific content, applications or services, or a combination thereof; (iii) the optimisation is objectively necessary to meet requirements for a specific level of quality; (iv) the network capacity must be sufficient to provide the specialised service in addition to any IAS provided; and the (v) specialised service must not be offered to the detriment of the availability or general quality of the IAS for end-users.

In this regard, two main points of concerns rely upon (i) uncertainty possibly created by the current case-by-case approach embraced by the BEREC guidelines, and (ii) possible restrictive interpretation of the criteria concerning the detriment for the general quality of the IAS for end-users. As for the impact on the quality of internet, there is no clear definition of what is meant by 'general quality of IAS' and what the minimum standard expected is in an 'open internet' context. Moreover, it must be noted that this kind of regulation (definition of minimum quality) does not consider at all the competitive dynamic among ISPs, and whether a detriment of the internet general quality may have

[168] European Commission (2023) Report on the implementation of the open internet access provisions of Regulation (EU) 2015/2120 – COM (2023) 233 final.
[169] To clarify, it is worth mentioning the difference between two of the main distinctions in regulation theory: (i) rules under proportionality principal vs rules under precaution principle, as mentioned above, and (ii) principle-based rules vs detailed rules, as mentioned here. The former refers to the generality of rules, that is the range of possible interpretations and their need of (ex-ante or ex-post) specification to be applied, whereas the latter refers to their restrictiveness, that is the ranges of licit (and illicit) behaviours. Those are interlinked, yet different concepts.
[170] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, BoR (16) 127, and afterwards BoR (20) 112, and lately BoR (22) 81.
[171] European Commission (2023) Report on the implementation of the open internet access provisions of Regulation (EU) 2015/2120 – COM (2023) 233 final.
[172] Ofcom – Net Neutrality review – Statement, 26 October 2023.
[173] Art 3(5) OIAR.

an impact on the end-user's choice and demand, as far as IAS are concerned. On the contrary, the rules in force, and their interpretation, are designed as a typical quality regulation in a monopoly, aimed to strictly protect end-users who have no alternative choices but to be subject to a degradation of quality, as if decades of pro-competitive regulation haven't had any effect.

In order to move away from this approach, it is necessary that consumers are properly empowered (as described in section 2) and informed and thus could use their power to react and sanction quality variation for their services. Also, because, presumably, highly specialised services will be developed in areas where there is high demand and business-cases find possibility to remunerate investments, and thus a higher level of competition. Therefore, incentivising companies to develop quality competition, rather than (only) price competition with a minimum quality standard would allow to move away from a commoditisation of the industry, as instead the current approach has been leading for the last years.

3.4 Policy Recommendations

3.4.1. Updating at the EU level net neutrality rules interpretation

In order to address the legal uncertainty and unknown compliance risks that could limit operator incentives to develop innovation, some further centralised guidance seems to be necessary. Legal uncertainty would not only represent a potential hold back for ISP industry yet would imply a consequent risk of diverging approaches to application of the net neutrality rules at national level. This risk is going to increase in time, as the 'industrial internet' use-cases develops on the back of new network infrastructures.

For this reason, it seems preferable to **develop centralised guidance from the Commission with a broader integrated policy view, possibly in the form of a recommendation**. Within the EECC, the Commission can issue harmonisation recommendation (Article 38 EECC), whereas it is not empowered with specific harmonisation tools under OIAR. Nevertheless, the Commission may issue recommendations under art. 292 TFEU to ensure harmonised application of EU legislation. At this aim, the Commission should undertake a thorough empirical study about the impact of NN rules on market and innovation dynamics, which should inform its harmonisation and guidance approach within the Recommendation.

3.4.2. Amending net neutrality regulation

Despite a further and enhanced harmonisation and guidance, should the evolution of technology and market make current rules inadequate, posing a risk for the deployment and exploitation of new technologies, a more **radical rethinking of OIAR rules should be considered. As mentioned, this should be done according to principles of ne[x]t neutrality: proportionality, systemic perspective, and end-user's empowerment**.

In this respect, policy makers should anyway consider that intense competition among ISPs tends to provide a safeguard against severe rent extraction and, thus, an abuse of throttling as an exploitative device, as showed by the above-mentioned economic analysis. Therefore, enforcement of NN rules should always account for the competitive environment, under a proportionality approach. As a general concept, updating NN rules would allow possibilities to differentiate quality which could be

beneficial for ISPs, as giving room to move away from pure price competition and allow consumers wider choices for better matching their preferences. Of course, any possible negative impact on the evolution of innovative content service should be considered.

One interesting reference about updating NN obligations is given by the recent Ofcom statement.[174] In this line, Ofcom underlines that ISPs should be able to offer **premium quality services**, at a premium price, differentiated from standard quality ones, at a more affordable price, in order to better meet differentiated costumers' needs (i.e., customers using high-quality virtual reality application vs users that only browse the internet). This is in line with the current BEREC concept of 'application-agnostic offer', as this differentiation applies to all the content and services accessed by consumers purchasing the offer. ISPs should be also probably allowed to indicate that all content and application with certain characteristic (e.g., on demand video streaming at very-high definition, 4k) could be available only with some premium package, therefore linking it to the concept of "*objectively different technical QoS requirement of traffic categories*". If those categories of traffic are related with "premium" content/service, charging an additional price to users, a commercial equilibrium between the IAS and Content/Application prices for users could be found – even by possibly framing and considering the differential premium service as a particular form of Premium Rate Service (PRS).[175]

Moreover, in its statement, Ofcom **allows zero-rating offers that are genuinely open** to all content providers offering similar services and contents ("class-based offers"), e.g., video streaming content, audio streaming content or social media. Further to that, ISPs should be probably allowed to build retail offers where specific content is treated differently ('**content-specific retail offers'**) when consumers choose for such a differentiation, selecting the specific content (that could be made available by CAP in a "premium" fashion).

As long as **customers truly have a choice** – i.e., a competitive market environment and the existence of a portfolio of tariff options and comparable plan where all content is unthrottled or not blocked – consumers could be allowed to voluntarily opt for differentiating certain traffic categories.[176]A simple solution could be to **introduce an application-agnostic 'anchor product' with a minimum QoS and which all users can choose** if they want. With that in place, ISPs can offer all type of differentiated services in addition to that, without affecting, yet enhancing, consumers' freedom of choice. If users expressly choose those alternatives, it means they are better off than with the anchor product. This approach should prevail over the concept of compulsory application-agnostic offer, which at the end could be limit consumer sovereignty and empowerment, not allowing them to reach those contents with that differentiated quality they would prefer. In other words, there is a trade-off between article 3(1) and art 3(3) of OIAR, requiring some balancing and a consumer-empowering approach to NN seems a balanced solution allowing to reach the most efficient outcome.

In this regard, it seems important to underline that the same art 3(1) of the OIAR gives end-users the possibility to choose for their own terminal equipment,[177] which has been considered a fundamental

[174] Ofcom – Net Neutrality review – Statement, 26 October 2023.
[175] About PRS: https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/premium-rate-services.
[176] Kramer J, Peitz M (2018).
[177] That is the equipment directly or indirectly connected to the interface of a public network. This interface, the Network Termination Point (NTP), is defined as the physical point at which a subscriber is provided with access to a public communications network. The location of the NTP has an impact on whether the router and modem are part of the ISPs' network or end-users can use their own equipment to access the Internet. In this regard, abovementioned BEREC guidelines

element of net neutrality. Therefore, it would be quite incoherent to consider end-users to be so sophisticated and well informed to take advantage from a personal choice of a terminal equipment (if they prefer not to buy and use the default standard product supplied by ISPs), while, at the same time, considering in a negative way a possibility for them to choose how their connection could be configured in terms of type of traffic and prioritisation (should they want to have another configuration).

This consumer-empowering approach to net neutrality should be **possible also for zero-rating** practices when the end-users select the applications or contents for which data usage is not subtracted from his data allowance. This selection should be transparent and non-discriminatory meaning that all contents and applications could be potentially chosen by end-users for the "premium" treatment. If access to zero-rated partner programmes is non-discriminatory and entails low barriers to entry, a sound theory of harm for content providers will usually not be given.[178]

Finally, it is important to stress again that, in this consumer-empowering vision for NN, likewise for the general consumer empowerment, the **transparency** provisions are of paramount importance, yet (as previously highlighted) a unified approach with consumer empowerment rules in the EECC should be necessarily carried out.

3.4.3. Better framing the regulatory trade-offs between traffic management and investments

The core provisions relating to agreements for IAS and equal treatment of traffic can be found in Articles 3(2) and (3) of the Regulation, which respectively states that: (i) it is permissible for providers of IAS to enter into agreements with end-users with respect to the commercial and technical conditions of IAS, and (ii) traffic delivered over the IAS must be treated equally, other than in certain set circumstances. The existing guidelines from BEREC on this topic indicates that it is permissible for ISPs to offer different tiers of IAS, based on parameters such as volume or speed or other Quality of Service (QoS) parameters (e.g. latency, jitter). This is provided they remain application-agnostic within the specific IAS i.e. the commercial and technical treatment of traffic is independent of application.

However, **in order to operate effectively and ensure that a higher tier internet access service is maintained, in certain circumstance it may be necessary to apply traffic management** measures to differentiate between the different tiers of service. Specifically, in times of congestion, it may be necessary to apply traffic management to ensure contractual commitments for the higher quality services are met. The current guidelines do not explicitly confirm that such an approach to traffic management would be permissible. Current NN rules and guidelines allow "reasonable" traffic management practices, that are transparent, non-discriminatory, and proportionate, and not based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic (art 3.3 OIAR). ISPs are allowed to go beyond reasonable traffic management if necessary and only for as long as necessary, in order to prevent network congestion and mitigate the effects of exceptional or temporary network congestion, provided that equivalent

on the Implementation of the Open Internet Regulation have dealt with this issue, and in addition, more specifically, also BEREC Report on the Location of the Network Termination Point - BoR (18) 159, and BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies - BoR (20) 46.

[178] Kramer, Peitz (2018).

categories of traffic are treated equally. Therefore, according to BEREC guidelines, when there is recurrent and more long-lasting network congestion, ISPs cannot apply traffic management practices but have an obligation to invest in order to expand their network capacity.[179]

In this regard it should be highlighted that installing more network capacity just to handle peak load traffic leads to significant social costs[180] as well as private costs for the ISPs.[181] It may be that in a growing traffic scenario overprovision could be the necessary industrial strategy, yet network operators would anyway be more efficient if allowed to manage traffic more freely. Consequently, in competitive markets, an efficiency rationale for the use of permanent traffic management practices that cater to a certain category of content could be allowed. Or, in alternative, those CAPs (co)causing congestion (negative externalities) should be called to contribute to their internalisation, either by mandating a financial contribution to a fund or also trough a (co)investment.[182]

In Italy, in order to avoid network congestion resulting from traffic peaks and a degradation of quality of service for all internet customers, the national regulatory authority AGCOM required DAZN, which broadcasts "Serie A" football matches over the internet, to provide ISPs with equipment to be integrated into their networks to handle a substantial share of the overall DAZN-originated live streaming data traffic.[183] AGCOM's decision aimed to preserve network integrity and protect consumers, yet this could not be based and refer to the current net neutrality rules. In making this order AGCOM, giving an extensive interpretation of some Code provisions, considered the CDN as subject to the electronic communications code, including the general authorisation regime.[184]

This anecdotal episode seems to represent the facts that NN rules may constitute an obstacle to address (positive, or, as in this case, negative) externalities in the wider digital ecosystem. Therefore, should NN rules be considered not amendable (or also in conjunction), it seems efficient and fair to introduce additional rules imposing, under certain specific circumstances, to other **actors in the extended telecom value chain obligation to contribute to the ecosystem, either co-investing or contributing to an investment fund** (as discussed in the next section 4). Investment in network capacity is extremely important for the open internet objectives: specialised services can be more easily developed. The impact on the overall quality of IAS for end-users depends on the overall network quality and the investments undertaken. Therefore, the need to upgrade the networks is strictly related to the possibility for companies to exploit the technologies while maintaining an overall high-quality standard.

[179] BEREC 2022 NN guidelines, para 93.
[180] Kramer, Peitz (2018) For example, because more cell towers need to be installed in somebody's neighbourhood (often appealed by citizen's initiatives), higher energy consumption and more electromagnetic interference.
[181] This is particularly true for MNOs for which part of the roll-out costs are induced by traffic, while for fixed lines most network costs are induced by coverage and not by traffic. However, we are dealing here with situations of potential network congestions, where additional investment for addressing peak load traffic cannot be unrelated to traffic.
[182] As previously highlighted, within the internet ecosystem, there are large difference between CAPs. For example, traffic from cloud services is largely balanced and mostly happens off-peak.
[183] AGCOM decision n. 206/21/CONS.
[184] Afterwards, a government's legal provision gave AGCOM's decision a more solid legal basis.

4. A Coherent Framework for Universal Service and Connectivity Targets

4.1 Current Regulatory and Policy Approach(es)

4.1.1. Universal service rules

Universal service (US) is a policy aimed to allow all citizens to have access to certain essential services, throughout the national territory with a 'adequate' level of quality. Therefore, universal service is a social regulation as primarily concerned to avoid exclusion. However, the universal service policy does not only satisfy individual needs, but also collective ones, since it represents a key factor for promoting economic and social cohesion, which is one of the main functions assigned by EU legislation to services of general interest.

Currently, within the EECC, Universal service is finalised to provide an adequate broadband service at affordable price.[185] Indeed, after liberalisation, EU regulation has been focusing on the universal service as a safety net to ensure that at least a set of the minimum services are available to all end-users. Currently, the minimum set of services which adequate broadband IAS must be at least capable of supporting are listed at Annex V of the EECC. In this respect, the US applies to widely adopted technologies, because it was assumed that the risk of 'exclusion' arises only when one person cannot access technologies which most of the population have. That's also why the definition of adequate broadband IAS by each MS for end-users is supported by the periodic BEREC reports, which assess Member States' current best practices.[186]

Although Member States are empowered for the actual definition of 'adequate' broadband services, this approach is therefore assuming (for the great majority of circumstances) that the network infrastructures necessary to provide those socially necessary services is already in place. Consequently, the current universal service policy (i) refers (only) to downstream services, by (ii) assuming that basic services (listed at Annex V of the EECC) are sufficient to grant social and economic inclusion and therefore, at the end, (iii) has a main focus on price affordability.[187] For this reason, NRAs have also duties to monitor retail prices of such services available on the market. Prices that are not affordable because consumers have low incomes or special social needs require affordability measures to be taken by NRAs, mainly by imposing providers of such services to offer to those consumers' tariff options or packages different from those provided under normal commercial conditions. [188]

[185] Art 84 and 85 EECC. The innovations introduced by the 2018 Code with respect to the previous regulatory framework are essentially limited to the revision of the scope of the US, explicitly including the provision of affordable broadband Internet access for all consumers (art. 84 EECC), as the concept of universal service must evolve to reflect advances in technology, market developments and changes in user demand (Recital 210) and exclusion of obsolete services such as public telephony and paper telephone directories.

[186] Art 84.3 EECC.

187 As for the last point (iii), NRAs must monitor the evolution and level of retail prices of such services available on the market. Prices that are not affordable because consumers have low incomes or special social needs require affordability measures to be taken by NRAs, mainly by requiring providers of such services to offer to those consumers tariff options or packages different from those provided under normal commercial conditions (Art. 85 CECE).

[188]Art. 85 EECC.

Member States can impose on companies appropriate Universal Service Obligations (USOs) to meet all reasonable requests by end-users for adequate broadband internet access service.[189] With regard to the definition of USOs, NRAs are entrusted with the task of designating the undertaking(s) responsible for providing universal service. If the net cost of the service obligations borne by the designated undertaking(s) is deemed to be excessively high, NRAs may introduce a compensation mechanism in favour of that provider, financed through public funds, or by distributing that cost over all providers of electronic communications services).[190]

4.1.2. Connectivity targets

With emergence of new technologies, the public policy debate about electronic communications markets began to gradually focus on industrial policy issues, such as the extensive development of future-proof technological assets. The EU and its Member States progressively designed industrial policies for new investments, by setting connectivity and ultra-broadband targets. At the European level, these industrial policies have been raised from the goals established within the 2010 Digital Agenda for Europe (DAE)[191] to the ambitious objectives within the 2016 Gigabit Society (GS).[192] In the 2016 GS, the Commission set out the following connectivity objectives for 2025: (a) all Union households, rural or urban, should have an internet connectivity with a download speed of at least 100 Mbps, upgradable to 1 Gbps; (b) socio-economic drivers, such as digitally intensive enterprises, schools, hospitals and public administration should benefit from a download speed of at least 1 Gbps and an upload speed of at least 1 Gbps; and (c) all urban areas and major transport paths should have uninterrupted 5G coverage.

Within this context, an important question concerned the rationale and incentives for the industry to invest in enhanced connectivity. Some investments are driven by competition dynamics incentivised by the pro-competitive regulation, in order to provide better services and differentiate from competitors. Moreover, investments targets set by EU institutions, even if not compulsory,[193] have represented a 'reverse-focal point'[194] for companies toward which to converge because of the competitive dynamics in place (and also political moral suasion).

Nevertheless, **to pursue such highly ambitious objectives and address their challenges, new regulatory approaches were progressively developed**, both identifying the deployment of Very High-

[189] Art 86 EECC.
[190] Art. 89-90 EECC.
[191] European Commission (2010). Communication on A Digital Agenda for Europe—COM (2010) 0245.
[192] European Commission (2016). Communication on Connectivity for a Competitive Digital Single Market—Towards a European Gigabit Society— COM (2016) 587 Final.
[193] Even if the investment targets are not formally compulsory neither for companies nor for member states, as defined as non-binding soft-law acts, those targets have progressively assumed some compulsory features for Members States. First, RRP loans have been conditioned to the obtainment of the 2030 targets (sometimes anticipated compared to 2030). Moreover, the (i) Decision (EU) 2022/2481 establishing the Digital Decade Policy Programme 2030, (ii) the Communication establishing the Union-level projected trajectories for the digital targets, (iii) the Implementing decision setting out key performance indicators to measure the progress towards the digital targets, and (iv) the Guidance to the Member States on the preparation of the national Digital Decade strategic roadmaps have built monitoring, "name and shame" and recommendation mechanisms to guide and push member states and their companies to reach those targets.
[194] In game theory, a focal point (a.k.a. *Schelling point*) is a solution that players tend to adopt in the absence of communication because it appears relevant to them. Schelling describes a focal point as: "*each player's expectation of what others expect him to do*". Usually, this is a solution aimed to avoid a coordination failure, as it happens in the prisoner dilemma on which the concept of competition is based. Here, we define a "reverse" focal point as a progressive convergence point of competitive dynamics, which enhance competition (via quality-enhancing investments) rather than eliminating it.

Capacity Networks (VHCN) as a formal objective of regulatory framework and adapting the existing regulatory tools, e.g., with regards of access regulation, co-investments, and reduction of deployment costs.[195] In addition, Member States have developed extensive national policy plans to stimulate ultra-broadband rollout through public funding from either national or EU resources. As a complement, the investment targets have been recently taken as general reference within the 2023 Broadband state aid guidelines, for triggering and justifying state aids intervention.[196]

Notwithstanding this evolutionary regulatory context, Universal service rules hasn't been subject to any substantive adaptation, although the industrial policy objectives have been motivated and based on 'universal' societal and economic needs. The 2021 Digital Compass communication states that "*it is our proposed level of ambition that by 2030 all European households will be covered by a Gigabit network, with all populated areas covered by 5G*".[197] Likewise, the Decision establishing the Digital Decade Policy Programme 2030 (DDPP)[198] underlined that "*Societal needs for converging upload and download bandwidth are constantly growing. By 2030, networks with gigabit speeds should become available to those who need or wish to have such capacity. All Union end-users should be able to use gigabit services provided by networks at a fixed location deployed up to the network termination point. Moreover, all populated areas should be covered by a next-generation wireless high-speed network with performance at least equivalent to that of 5G.*"[199] The 2024 White paper affirms that "*from a societal perspective, the availability of high-quality, reliable and secure connectivity for everybody and everywhere in the Union, including in rural and remote areas, is indispensable*".[200]

4.1.3. Divergence between industrial policy (connectivity targets) and Universal service regulation

Those recent EU communications and decisions are setting (in a dynamic perspective) a clear and strong universal service policy. Even though, however, it is not formalised and shaped very differently from the current conceptualisation of universal service rules, as detailed in the EECC. That conceptualisation of Universal service was indeed adequate for the post-liberalisation era, when the US framework was established to grant a safety net in a competitive environment, aimed not have liberalisation resulting in a withdrawal (or downgrading) of the services in certain areas. On the contrary, **it seems less fit for today's end-users needs**. First, the market dynamics and competition

[195] In September 2010, the Recommendation on the Next Generation Access Network; in 2013, a Recommendation on non-discrimination and costing methodologies; in 2014, the Cost-reduction Directive; finally, within the 2018 EECC, VHCN investment promotion has become a new independent general objective of the European strategy - art 3 (2) EECC. In particular, there are some specific EECC provisions that NRAs have to apply to shape this new balance between competition enhancement and investment promotion, e.g., Art 72: imposition of obligations on undertakings to meet reasonable requests for access to civil engineering assets; Art 61(3,4): Symmetric regulation; art 3(4), 73 and 74: better remuneration of investments ("reasonable rate of return") and adequate consideration of investment risk; art 16 and 79: promoting co-investments in VHCN by de-regulating (removing all access obligations) SMP operators who committed to an open offer for co-investments. See Manganelli A, Nicita A (2020).

[196] EC Communication - Guidelines on State aid for broadband networks (2023/C 36/01). Within the new Guidelines, the thresholds for intervention have been revised. Member States can support investment in fixed networks in areas where the market is not likely to provide end-users with a download speed of at least 1 Gbps and an upload speed of at least 150 Mbps. For the first time, the guidelines also provide a framework for the assessment of aid to the deployment of mobile networks (including 5G) and take-up measures.

[197] European Commission (2021) Digital Compass 2030, The European way for the Digital Decade – COM 2021/118 final.

[198] Decision (EU) 2022/2481 establishing the Digital Decade Policy Programme 2030.

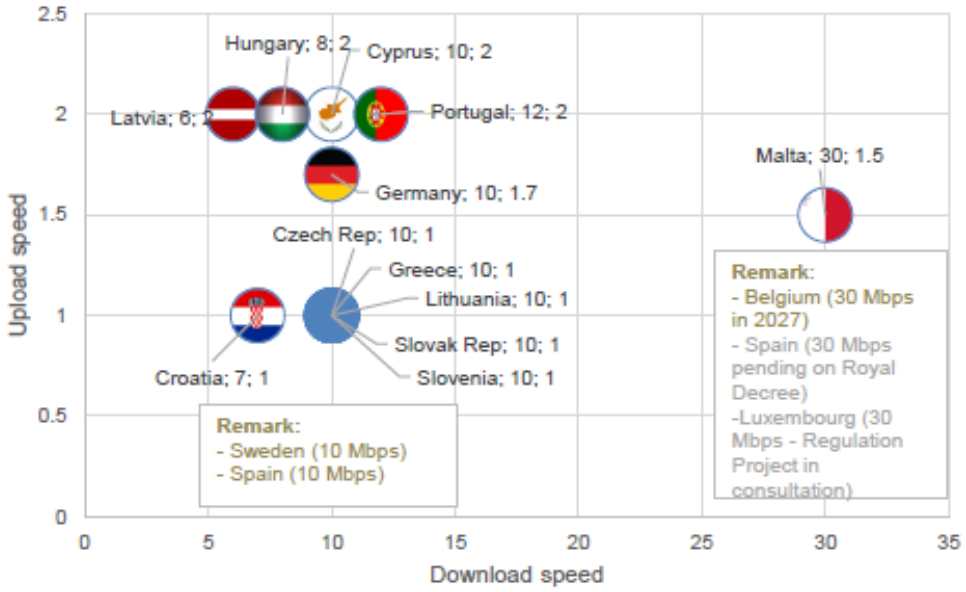
[199] Recital (7) and art 4.1.(2) (a) Decision 2022/2481.

[200] European Commission (2024), White paper.

largely resolved most of the affordability problems (especially with emergence of pre-paid mobile) for basic services. Second, basic connectivity is almost everywhere available.

In this context, art 86 EECC ('Availability of Universal service') which empower Member States to impose on companies appropriate Universal Service Obligations (USOs) to meet all reasonable requests by end-users for adequate broadband internet access service (and for voice communications services), has become marginal precisely because of the backward-looking regulatory conceptualisation of what are the necessary service. As for the actual current definition of the 'adequate BB IAS', not all MS have already defined it. Among those countries having set a definition, there is a moderate convergence toward 10 Mbps yet resulting in a growing heterogeneity (table 8). For example, Italy is targeting 20 Mbps, Malta, Belgium, Spain are targeting 30 Mbps, and Norway, where Parliament has defined a goal for a fixed broadband speed of 100 Mbps for everyone.[201]

Table 8 – Definition of "adequate BB internet access services" (BEREC 2023)



The reason of this increasing heterogeneity, that can't be justified with differentiated technical need to support the same minimum set of services defined in the Code's annex, is that national policy makers are starting to adopt a forward-looking perspective.

The contrast between the regulatory conceptualisation of universal service and the current policy framework is striking, especially considering the inherent affinity of these two public interventions. Both policies are based on a subsidiary role of the public intervention, to be triggered only where private investments are insufficient to meet end-users' connectivity needs, yet they are completely uncoordinated and animated by completely different rationales. According to the current EU policy vision, projected to 2030, 'being excluded' means not being reached by VHCNs. Consistently, any unavailability of adequate service (under art 86), should it require investment for new infrastructures, very unlikely would be remedied with an obligation to deploy network merely sufficient to provide basic services.

[201] BEREC report on 'Member States' best practices to support the defining of adequate broadband internet access service' BoR (23) 178.

This seems calls for an in-depth assessment about a **redefinition of the universal service policy, to be coordinated and consistent with industrial policy and connectivity targets**, and the existing state aids programmes.

4.2 What to be Assessed

4.2.1. Positive externalities and desirability of connectivity targets

The ambitious connectivity targets and the consequent public funding devoted to augmenting private companies' investment capacity are based on the assumption that "*there is a link between the increased deployment of fixed and mobile broadband and economic development … higher speeds and new generations of mobile networks have a positive impact on GDP*. "[202] So, the current EU industrial policy assumes that there are positive externalities across the digital ecosystem correlated with the deployment and provision of electronic communications networks. Some empirical economic studies supporting this general proposition.[203] However, most of the existing literature do not refer to VHCN connectivity and/or correlate most of benefits to a certain level of adoption.[204] Therefore there are contrasting opinions about the overall social benefit, and positive externalities, deriving from the Commission's targets and whether this justifies the costs, public and private, of achieving such objectives, particularly when it comes to remote and rural areas.

For this reason, it is to **recommend for the EU commission to undertake extensive empirical studies, using the most recent data regarding VHCN deployment, in order to give more clarity about the evidence-based foundations of its policy**. In this analysis, it must be considered a dynamic and forward-looking approach that such an industrial policy would embrace, so, on one side taking into account opportunity cost that could emerge from not adopting newer/alternative technologies (potentially outperforming current ones in terms of deployment costs/consumers' benefits) and, on

[202] EU Commission (2024), White paper.

[203] Quite a few analyses recognise a positive causal effect of the deployment of telecommunications networks and services on GDP growth. [Roller LH, Waverman, L (2001); Czernich N, Falck O, Kretschmer T, Woessmann L (2011)] Recent studies, specific to fibre investments in Italy, have shown that the use of ultra-fast connections has positive effects on both the productivity of firms [Cambini C., Grinza E. Sabatino L (2023)] and on market dynamics, favouring the entry of new firms in sectors with greater use of digital technologies. [Cambini C, Sabatino L (2023)] Therefore, socioeconomic benefits in terms of economic growth, productivity, as well as economic resilience, are high but are also subject to diminishing returns beyond a certain broadband quality level and the positive socioeconomic effects take hold only after broadband adoption on the demand side, but not with mere availability on the supply side. [Briglauer W and Grajek K (2023); Briglauer W, Kramer J, Palan N (2024)].

[204] Most of analysis quoted in the footnote # 2 in the "white paper" relates to instances in which end users were unconnected or connected to very low bandwidth connections and are ulteriorly connected to functional broadband (still <100Mbps). Most of them are empirical studies based on data up to 2012 and therefore are not directly related with the Connectivity targets (as connectivity targets are not trying to increase broadband penetration but rather achieve full EU-wide coverage to gigabit-capable networks). In this concerns, Koutroumpis P (2019) notes that "*while speeds are important for the efficient use of broadband, there are limits to the actual use of higher speeds on the economy […] I identify the limits beyond which further increases have a zero or negative effect on the economy […] I find that these speed thresholds exist and they, in fact increase over time, from 3Mbps in 2011 to 9.8Mbps in 2016*." Moreover, Liu Y-H, Prince J, Wallsten S (2018) find that "households' valuation of bandwidth is highly concave, with relatively little added value beyond 100 Mbps". Most importantly, the existence of positive externalities is not a sound basis for policy intervention, unless these externalities exceed the costs of such policies. On this, Briglauer W, Gugler K (2019) conclude that there are marginal benefits from full EU-wide fibre coverage and that "cost-benefit analysis implies that policy intervention – as foreseen by the European Commission – is only justified for coverage and adoption levels of around 50 per cent, whereas for a 100 per cent coverage level net losses are likely".

the other side, considering also future benefits and market developments (both on demand and supply sides) - which often justify a supply-driven approach, not at all unusual for the deployment of general interest infrastructures.

4.2.2. Relevant ecosystem: benefits and contributions

Within the current EU policy, in a scenario where connectivity targets have been justified and confirmed, it is assumed that there are positive externalities deriving from deployment of VHCNs. Positive externalities imply indirect benefits to individuals/companies for which the externalities' producers are not compensated because those benefits are external to the market(s) where that producers operate. In other words, private benefits (for the actors in the market considered) are lower than social benefits (outside that market) and therefore there is an under-provision of that service/goods. To realign social and private benefits, the activity producing positive externalities should be incentivised and increased, by internalising those positive externalities.

In this regard, another main aspect covered both by the recent 'White paper' and previous 'Exploratory consultation" on the future of the electronic communications sector and its infrastructure'[205] refers to the importance of defining a wider digital ecosystem, and therefore the interdependencies and the dynamics taking place within an extended value chain for digital networks and digital communications services. Therefore, it is important for any public intervention to **assess the magnitude of those positive externalities and also how they are distributed; in other words, what kind of subjects / companies are enjoying those externalities and whether and how the same subjects otherwise contribute to the ecosystem**.

In order to do that it is necessary to define: (i) what is the digital ecosystem, therefore what is the scope of markets and services which base their activity on the telecom infrastructure and enjoy positive spill overs from enhanced connectivity;[206] (ii) what is their exploitation of those benefits; and (iii) how much they contribute to the ecosystem. The recent EC exploratory consultation[207] had apparently a similar general objective, yet the outcome of the consultation did not reveal any concrete assessment. The same direction, as far as the contribution to the ecosystem is concerned, has been taken, much more concretely, by a recent draft BEREC report.[208] This framework would be coherent with a combined reading of provisions included in the (i) White Paper, and (ii) the European Declaration on Digital Rights and Principles for the Digital Decade, as follows: "*This new model of network and service provision relies not only on traditional electronic communications equipment, network and service providers but also on a complex ecosystem of cloud, edge, content, software and component suppliers, amongst others. The traditional boundaries between these various actors are increasingly blurred …*"[209] This requires "*adequate frameworks so that all market actors benefiting from the digital transformation assume their social responsibilities and make a fair and proportionate contribution to the costs of public goods, services and infrastructures, for the benefit of all people living*

[205] European Commission (2023) Exploratory consultation on the future of the electronic communications sector and its infrastructure.
[206] Above a certain level – as telecom networks are triggers for a multitude of services.
[207] European Commission (2023) Exploratory consultation.
[208] BEREC Draft Report on the entry of large content and application providers into the markets for electronic communications networks and services - BoR (24) 51. This builds upon a previous report focusing on the scope of the ecosystem: BEREC Report on the Internet Ecosystem - BoR (22) 167.
[209] European Commission (2024), White Paper.

in the EU."[210]The stepping stone of this revised policy approach would be to define an extended electronic communications value chain (a digital communications networks and services ecosystem) thus moving from a 'definition of relevant markets' to a 'definition of the relevant ecosystem'.

Once the relevant ecosystem has been defined, in theory, positive externalities could be tackled either: (i) '*à la Coase'*, i.e., by reducing transaction costs and letting the parties within the ecosystem to freely negotiate or (ii) '*à la Pigou'*, i.e., by providing subsidies aimed at internalising those externalities and re-align social and private benefits in an efficient outcome.

As described in the previous section, net neutrality rules, given the current market conditions, create insurmountable transaction costs within the ecosystem by qualifying several of the possible transactions between telcos and CAPs as illicit, thus making it very difficult to use Coesian market-based solutions. As proposed, a substantial rethinking and softening of the transactional constraints imposed by net neutrality rules would allow using certain market mechanisms to address externalities and therefore tackle under-provision of (network) services. In **a scenario where net neutrality legislation is not amendable, subsidies would be the only available solution to obtain an efficient outcome** (i.e., minimise under-provision). This could take the form of a fund channelling public money (as it has happened so far) and/or contributions from all market players that rely on the network infrastructures (making an intensive use of it) and exploit the correlated positive externalities.[211]

So, a regulatory/policy approach aimed at efficiently incentivising the ubiquitous deployment of networks should first define the relevant ecosystem. The definition of the relevant ecosystem would thus represent a preliminary regulatory tool, aiming to define the boundary within which is efficient and fair that externalities are compensated (internalised into the ecosystem), as an alternative or a complement to public funding.

At this aim, under a proportionality principle, **all existing contributions from market actors of such an extended digital communications value chain ("relevant ecosystem") should be taken into duly account**, as a mean to internalise positive externalities. These could be (i) actual network supplementary and complementary (co-)investments (including alternative broadband technologies and investments in infrastructure to deliver content to end-users) and/or (ii) indirect contribution to networks by stimulating the demand of internet access services through the provision of content. The former (i) is the easier to assess, although all data publicly available so far has been based on mismatching geographical area: the network investments from global CAPs are always considered on an overall global scale, whereas the Telcos' investments are accounted for on a nation-wide geographical basis. The latter point (ii) is the most problematic to assess and the most controversial.

Indeed, a complementarity between access and content weakens a "free riding" argument linked to a positive externalities' environment, as positive externalities are somehow reciprocal. Nevertheless, it should be considered that IAS subscriptions and digital contents are not perfect complements. This is mainly because, even if demand of connectivity is substantially driven by content consumption,[212] the

[210] European Declaration on Digital Rights and Principles for the Digital Decade.

[211] It seems worthwhile to specify that we are talking here about subsidies necessary to re-align private and social benefits (internalise positive externalities), that is subsidies aimed to cover those costs which are not rationale for market players to cover (consistently with state aids rules principles and rationales).

[212] A study by Deloitte (2024) includes a consumer survey and shows that end users demand IAS mostly to access content, with "basic services" representing little value for end users. https://research.ccianet.org/case-studies/estimating-value-content-applications-services-internet-users-europe/; moreover, a paper by Katz R, Jung J, Callorda F (2024) highlights that

decision for end-users to subscribe to an ISP (i) may come also from a few different reasons (e.g., interpersonal communications);[213] and (ii) is a preliminary (autonomous) choice in a two-step approach (whereas for typical complementary products users decide, at the same time, how much to buy in function of both products prices); and therefore (iii) the consumption of contents can be variable within a constant demand for connectivity.[214] Moreover, since the policy point is about enhancing the connectivity for Very High Capacity Networks, additional reasoning should be done about the quality of connectivity. Demand for contents increases as the quality of the network does, whereas that is not currently true for the IAS demand, which currently does not increase with the network quality. Therefore, telcos are not always necessarily able to charge end-users a higher connection charge for an enhanced connection quality (especially for non-business connections). This situation could be the result of highly competitive IAS market; however, this situation could also underline that there is no large incremental user's willingness to pay for the enhanced connectivity, thus signalling, again, that enhanced connectivity, and contents are not perfect complements.[215] Indeed, a low adoption on VHCN testify that the complementarity between the (currently available) contents and VHC IAS is low.

Again, this might also signal that the current EU industrial policy for connectivity targets is not well balanced and push away from situation where investments are done in a demand-driven approach (demand related to content). However, we are discussing here a scenario where those targets have been justified and confirmed, or, otherwise, revised.

4.3 Policy Recommendations

First, a **new definition of what needs to be considered an "adequate broadband internet access service" should be considered**, including also mobile internet access. This definition could be developed by the European Commission and/or BEREC in order to somehow aim at the connectivity targets, as dynamically and differentiated programmed by the strategic roadmaps and projected trajectories and KPI within the Digital Decade Policy Programme 2030. Moreover, it should be clearly distinguished between the 'universal' provision of connectivity and the provision of service, which would also enable to consider the fact that the market structure is undergoing substantial evolution, with an increasing delayering and, in some markets, separation between network/connectivity and services.

Second, after having performed a thorough cost/benefit analysis, it should be considered the **establishment of a fund to which all players in the digital ecosystem would contribute, as an alternative or complement to public funding (state aids),** for those costs which cannot reasonably be borne by private market actors, and which are not covered by public subsidies. In this scenario, allocation of USOs (and consequently of funds) to companies should be done through transparent

VOD services have been a key contributor to the increase of broadband connectivity and that VOD service offers have been associated with a gradual increase in the purchasing of broadband higher speed plans.

[213] Therefore, the cross-elasticity of demand not necessarily is always symmetric, that is, if the demand of all contents may decline when connectivity prices increase (because connectivity demand declines), not necessarily the demand of connectivity declines when the price of contents increase.

[214] Therefore, in case of a price increase for contents there will be less consumption of contents and not necessarily also a decline in the IAS demand. Symmetrically, when a decrease in contents price takes place, this will not be necessarily followed by an increase in connectivity demand yet rather an increase in content demand.

[215] Otherwise, any increase in consumer surplus on the content market should translate in a higher willingness to pay for connectivity.

procedures, possibly designating a variety of companies (as the EECC already foreseen, yet not applied). Contributions from that fund should be used either to invest in areas where there are no adequate infrastructures in place, considering the update definition of universal service and the related "technological market failures", and also where investment and upgrades are needed in order to avoid congestion because of increased traffic. At the end, this regulatory setting is not so faraway to what current USOs and US funds aim to do yet those current rules only cover a universal provision of very basic services and impose contribution obligations only to telcos operators.

Third, in this context, it seems crucial to consider whether competition has exerted a sufficient downward pressure on prices resulting in a general affordability of services that would support **eliminating obligations to offer special tariffs or packages**; otherwise, **especially for VHCN affordability, consider allocating resources from the fund to support the demand of consumers with low income or special needs**. This is somehow the path already defined by the Code: "*Providing those consumers with direct support for communication purposes, which could be part of social allowances or vouchers for, or direct payments to, those consumers. This can be an appropriate alternative having regard to the need to minimise market distortions*."[216] In this convergent path, the 2023 revised Broadband state aid guidelines, for the first time provide a framework for the assessment of demand-side measures, explicitly considering "social vouchers" (highlighting the converging trend between Universal Service and State Aids). This of course would become an interesting tool once adequate broadband services is defined according to the policy target, since would allow to design ***social vouchers*** **for VHCN services** to support households unable to fund the ongoing costs of that connectivity.[217]

An additional overarching recommendation is devoted to **connectivity targets and supply-driven approach, in order to seek and maintain a balance with the demand evolution**. In this concern, it might be worthwhile discussing about some mechanisms making the subsidies for VHCN coverage extension contingent upon a minimum level of end-customers VHCN subscription and/or commitment to subscribe to a VHCN tariff. In this same direction, a **greater attention should be devoted on the role of public intervention in sustaining the demand**, focusing on means of stimulating 'collective demand' as e-government, e-education, e-health services. Similarly, it would be worthwhile exploring connectivity vouchers to sustain "collective purchasing programmes", organised and administered by local authorities or non-profit bodies, to promote collective adoption of VHCN. [218]

[216] Recital 219 EECC.

[217] Bourreau M, Feasey R, Hoernig S (2017).

[218] For the first time, the 2023 Broadband State aids guidelines provide a framework to assess demand-side measures, not only for social purposes (as highlighted previously), yet mainly to address specific market failure in terms of take-up of available broadband services ("connectivity voucher"). Different means of implementation may be provided for under national rules. For instance, a connectivity voucher scheme may provide for payments directly to the end users or directly to the service provider chosen by the end users.

References

Allcott H, Sunstein C (2015) Regulating Internalities, Journal of Policy Analysis and Management, Vol 34, Issue3, 698-705.

Analysys Mason (2022) The impact of tech companies' network investment on the economics of broadband ISPs, October 2022

Arthur D. Little (2023) The Evolution of Data Growth in Europe

BEREC Guidelines on the Implementation by National Regulators of EU Net Neutrality Rules - BoR (16) 127.

BEREC Report on the Location of the Network Termination Point - BoR (18) 159.

BEREC Guidelines on the Implementation of the Open Internet Regulation - BoR (20) 112

BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies - BoR (20) 46.

BEREC Report on the Interplay between the EECC and the EC's proposal for a Digital Markets Act concerning number-independent interpersonal communication services – BoR (21) 85.

BEREC Guidelines on the Implementation of the Open Internet Regulation - BoR (22) 81

BEREC Report on the Internet Ecosystem - BoR (22) 167.

BEREC report on interoperability of Number-Independent Interpersonal Communication Services (NI-ICS) – BoR (23) 92

BEREC Report on Member States' best practices to support the defining of adequate broadband internet access service - BoR (23) 178

BEREC Draft Report on the entry of large content and application providers into the markets for electronic communications networks and services - BoR (24) 51

BEREC Draft Report on the IP Interconnection ecosystem – BoR (24) 93.

Bourreau M, Feasey R, Hoernig S (2017) Demand-Side Policies to Accelerate the Transition to Ultrafast Broadband – CERRE Report.

Bourreau M, Kourandi F, Valletti T (2015) Net Neutrality with Competing Internet Platforms. Journal of Industrial Economics, 63(1), 30–73

Briglauer W (2024) Efficiency and Effectiveness of Net Neutrality Rules in the Mobile Sector: Relevant Developments and State of the Empirical Literature, available here

Briglauer W, Grajek M (2023) Effectiveness and efficiency of state aid for new broadband networks: evidence from OECD member states, Economics of Innovation and New Technology, 33(5), 672–700.

Briglauer W, Gugler K (2019) Go for Gigabit? First Evidence on Economic Benefits of Highspeed Broadband Technologies in Europe, in Journal of Common Market Studies, Volume 57, Number 5, 1071–1090.

Briglauer W, Kramer J, Palan N (2024) Socioeconomic benefits of high-speed broadband availability and service adoption: A survey, in Telecommunications Policy, Volume 48, Issue 7

Briglauer W., Gugler K., Cambini C., Stocker V. (2022) Net neutrality and high-speed broadband networks: evidence from OECD countries. European Journal of Law and Economics

Cambini C., Valletti T. (2005) Information Exchange and Competition in Communications Networks, Journal of Industrial Economics, LVI(4): 707-728.

Cambini C, Sabatino L (2023) Digital highways and firm turnover, in Journal of Economics and Management Strategy, 32(4), 673- 713.

Cambini C., Grinza E. e Sabatino L. (2023) Ultra-fast broadband access and productivity: Evidence from Italian firms, in International Journal of Industrial Organization, 86, 102901.

Cave M, Vogelsang I (2015) Net Neutrality: An E.U./U.S. Comparison. Competition Policy International, 11(1), 85–95

De Streel A, Sibony A-L (2017) Towards smarter consumer protection rules for the digital society – CERRE Report.

Deloitte (2024) Estimating the Value of Content and Applications Services for Internet Users in Europe

Economides N, Hermalin E (2015) The Strategic Use of Download Limits by a Monopoly Platform. RAND Journal of Economics, 46(2), 297–327.

Ericsson (2022) Mobility Report 2022

European Commission (2011) Staff working paper: Consumer empowerment in the EU - SEC (2011) 469 fin.

European Commission (2010) Communication on A Digital Agenda for Europe—COM (2010) 0245.

European Commission (2016) Communication on Connectivity for a Competitive Digital Single Market—Towards a European Gigabit Society— COM (2016) 587 Final.

European Commission (2020) market monitoring survey 2020 – internet provisions.

European Commission (2020) market monitoring survey 2020 – mobile services /internet provisions.

European Commission (2021) E-Communication in the Single Market [Special Eurobarometer No. 510, June 2021]

European Commission (2021) Digital Compass 2030, The European way for the Digital Decade – COM 2021/118 final

European Commission (2023) Exploratory consultation on the future of the electronic communications sector and its infrastructure

European Commission (2023) Report on the implementation of the open internet access provisions of Regulation (EU) 2015/2120 – COM (2023) 233 final

European Commission (2024) White paper on How to master Europe's digital infrastructure needs? COM (2024) 81 final

Fletcher A., Vasas Z. (2023) Implementing the DMA: The role of behavioural insights - forthcoming in Oxford Review of Economic Policy.

Garrett T., Setenareski L., Peres L., Bona L., Duarte E. (2022). A survey of network neutrality regulations worldwide. Computer Law & Security Review, 44

Greenstein S, Peitz M, Valletti T (2017) Net Neutrality: A Fast Lane to Understanding the Trade-Offs. Journal of Economic Perspectives, 30(2), 127–150

Katz R, Jung J, Callorda F (2024) The role of Video on Demand in stimulating broadband adoption, in Telecommunications Policy, Volume 48, Issue 4

Koutroumpis P (2019) The economic impact of broadband: Evidence from OECD countries, Technological Forecasting and Social Change, Volume 148

Kramer J, Peitz M (2018) A fresh look at zero-rating, Telecommunications Policy, Volume 42, Issue 7, 501-513.

Larouche P (2012) Network Neutrality: The Global Dimension (Eds. M. Burri & T. Cottier). Trade Governance in the Digital Age: World Trade Forum, pp. 91–122.

Liu Y-H, Prince J, Wallsten S (2018) Distinguishing bandwidth and latency in households' willingness-to-pay for broadband internet speed, Information Economics and Policy, Volume 45

Manganelli A, Nicita A (2020), The Governance of Telecom Markets, Palgrave MacMillan.

Manganelli A, Nicita A (2022) Regulating Digital Markets: the EU approach. Palgrave Macmillan.

Manganelli A, Schnurr D (2024) Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies – CERRE Report

Ofcom (2017) Review of the market for standalone landline telephone services

Ofcom (2023) Net Neutrality review – Statement, 26 October 2023

Ofcom (2023) Statement – Network Neutrality Review.

Roller LH, Waverman, L (2001) Telecommunications Infrastructure and Economic Development: A Simultaneous Approach. American Economic Review, 91(4), 909–923.

Czernich N, Falck O, Kretschmer T, Woessmann L (2011) Broadband Infrastructure and Economic Growth. The Economic Journal, 121(552), 505–532.

Sandvine (2023), Global Internet Phenomena Report

Stocker, V., Smaragdakis, G., Lehr, W.H. & Bauer, S. (2017) The Growing Complexity of Content Delivery Networks: Challenges and Implications for the Internet Ecosystem, Telecommunications Policy, 41(10), 1003-1016

TeleGeography (2023), The State of the Network, 2023 Edition, p. 10. Sandvine, Global Internet Phenomena Report, 2023

Wik (2021) Strategies to promote Over-the-air provisioning - Study for ComReg

Wu T (2003) Network Neutrality, Broadband Discrimination, 2 J. on Telecomm. & High Tech. L. 141

Yoo C (2023) Network slicing and net neutrality. Telecommunications Policy, Volume 48, Issue 2

cerre Centre on Regulation in Europe

TELECOMS RESILIENCE & SECURITY

PAUL TIMMERS

Executive Summary

Public policy to safeguard and strengthen resilience and security in the EU telecom ecosystem must address telecoms cyber/physical security, supply chain security, and economic security. At the same time, such a policy should enable the competitiveness of the EU telecoms sector. Resilience and security are an important business area and can be a key competitive differentiator for the telecom industry. Developing the required capabilities, capacities, and control will also enable EU telecoms to contribute to European strategic autonomy. Pursuing all these objectives (strengthening security, resilience, competitiveness, and strategic autonomy) is neither self-evident nor will it be possible to maximize all of them at the same time.

This study takes as context and baseline the State of Play chapter of the overall CERRE Telecom report. The present analysis moves through three perspectives. The first is an *internal perspective* on the telecom ecosystem as regards resilience and security. The conclusion is that the **telecom ecosystem does encounter significant resilience and security challenges yet has much experience in handling these and is fairly robust**. However, this may change with the structural transformation of the sector itself and important ongoing changes in its context.

The second perspective considers this context in terms of *external forces* that affect security and resilience in the telecom ecosystem. There are several of such forces and their impact can be negative but equally also positive. They range from geopolitical tensions to powerful new entrants, from transformative new technology to demanding new cybersecurity legislation. These forces drive towards significant transformation that will strongly impact resilience and security, creating new challenges and new opportunities. They **need to be addressed to avoid that both resilience/security and competitiveness deteriorate** in the longer term.

The third perspective focuses on *actors* and their motivations to try and influence these forces. Examples are concerns about economic security, pressure for increased capital returns, and political commitment to environmental sustainability. We need to understand these motivations in order to recommend policy that enables strengthening resilience/security as well as competitiveness yet is also realistic about possible trade-offs between these objectives.

This study does not conclude that from a security and resilience standpoint more legislation is needed, though **guidance is needed to ease navigating the regulatory landscape**. The report does, however, argue that more concrete action is necessary – and proposes such action – and importantly – and ambitiously - advocates a **more holistic approach to policy for telecoms resilience and security**.

The recommendations based on the analysis, are given below. They are detailed in the final chapter of this report. Concrete action is added to each recommendation to illustrate how to start implementing them and to encourage the suggested 'action holders' to do so.

Resilience and security must be tackled by integrated policy. This can be translated into concrete action. This is ambitious and but there is a need for transformational policy change.

Recommendation 1: pro-active engagement of policy makers and industry to develop **'holistic' EU telecoms resilience and security policy** that strengthens economic security/strategic autonomy and competitiveness.

***Action 1**: EC, EEAS, ENISA, Member States authorities together with industry to:*

- Select **priorities and perform a resilience and security end-to-end analysis** of the wider telecom ecosystem. An agenda of priorities comes from the present study and references from ENISA, 5G/6G development, international and national and industry guidance.
- Analyse the applicability of existing policy instruments and legislation and identify available options and choices; select these such that these **mutually reinforce** each other.
- In addition, the EC to provide **Recommendations to navigate the telecoms resilience and security regulatory landscape** and reinforce legal certainty; and to provide related training.

Specific recommendations relate to individual infrastructures. Action is being taken for subsea cables but is also needed for security of satellite systems/GPS, as well as IoT security within the telecom system.

Recommendation 2: certain **infrastructures (subsea cables, landing stations cable management systems, satellite systems, location services)** are a **high priority** for policy, with possible requirements for redundancy and fall-back networks and enhanced **cross-border cooperation** in the EU.

***Action 2**: similar to work on subsea cables by EC, ENISA, and NIS Cooperation Group, perform such analysis for the other priority infrastructures. Extend the involvement of actors beyond authorities and in line with Recommendation 1. Mobilise the full range of policy instruments where relevant. Develop guidance on the revised Network and Information Security Directive and the Cyber Resilience Act.*

Preparedness is needed for serious disruption such as by adversary states. This is ambitious yet action is indispensable. Though urgent this will inform longer-term multi-country, cross-border and cross-sectoral cooperation (e.g., electricity-telecom, civil-military), in line with Recommendation 1.

***Recommendation 3**: step up **telecoms cyber- and physical defence**, possibly preparing for war. This must be done coherently with broader policy discussions on defence and deterrence such as with NATO. Associated costs must be recouped in top line, bottom line, and public funding.*

***Action 3:** industry together with national and EU authorities to urgently perform **multi-operator and multi-country / cross-border / cross-sectoral exercises in disruption** and crisis management, fall-back and redundancy, leading to understanding of bottlenecks and lines of emergency*

communication. Consider raising public awareness raising. Involve the EU-CyCLONe network and EU Integrated Political Crisis Response. EC and Member States to put forward public funding.

Specific points of attention from the analysis are interoperability and redundancy:

Recommendation 4: address trade-offs between competition policy, market access policy, industrial policy, open strategic autonomy in considering **requirements for secure interoperability**. Also consider if **redundancy** with symmetric open access can improve resilience. Consider supporting redundancy by public co-financing.

***Action**: European Commission (DG-COMP) to develop guidance to assess where interoperability and open access requirements contribute to resilience and security of telecoms. DG-GROW, DG-RTD and DG-CNECT to provide requirements in Horizon R&D, Digital Europe, Connecting Europe for interoperability and open standards for resilience and security. Member States and EC to provide criteria for co-financing of redundancy in Cohesion and NextGenerationEU funding.*

Telecoms actors can and should have a role in defending global open economy and global collaboration for stability, safety and security of digital infrastructures.

Recommendation 5: pro-actively advocate **global collaboration on resilience and security** of telecom infrastructures and promote de-escalation in this context. Promote norms for the protection of transnational communications infrastructures.

***Action**: Industry to engage with Member States governments and EEAS to support them in international forums notably for UN Norms and cybersecurity capacity building, cyber-diplomacy training, international telecom infrastructure building in the EU's Global Gateway funding initiative.*

A focal point are international ICT supply chains, also for telecoms. It is not clear at this stage what precisely the economic impact is of de-risking. More impact assessment work is needed.

Recommendation 6: critically assess the **impact of different geo-economic strategies** (e.g., globalisation and regionalisation) on telecoms resilience and security.

***Action**: industry to urge EC to perform economic security risk assessment on telecoms ICT supply chains and launch itself a study and seek cooperation with ENISA and the NIS Cooperation Group to provide its inputs such as on regionalisation/reshoring vs globalisation/supplier diversification.*

On cross-cutting vs sectoral approaches:

Recommendation 7: anticipate the 2027 review of horizontal cybersecurity legislation aiming that this can address the telecom ecosystem in a system-wide approach; possibly with limited vertical

cybersecurity measures provided consistency is strictly maintained (using experience from finance and energy); insist on increased harmonization, being realistic about national security prerogatives.

Action: industry across the telecoms ecosystem to collaborate, if needed in a separate taskforce, to systematically follow the implementation of NIS2 and other horizontal cybersecurity legislation, as well as EECC, and compare with counterparts in electricity and financial/banking, for a reasoned opinion on future horizontal cybersecurity and resilience legislation. Combined with the guidance on current legislation (action from Recommendation 1) this can include simplification of legislation.

Finally, complementing legacy decommissioning as an important theme in the Sustainability Report:

Recommendation 8: policies to **decommission legacy equipment** and networks should also be motivated by security concerns. Nevertheless, if legacy is kept in place for reasons of resilience, guarantees should be provided for reliability, availability, and coverage.

1. Introduction

The objective of this report is to provide actionable policy recommendations on security and resilience that safeguard or strengthen resilience and security; strengthen the competitive position of the European telecoms industry; and more generally, advance EU telecoms economic security and strategic autonomy. The recommendations address a broad and longer-term perspective on security and resilience in line with the orientation of the overall CERRE Telecom project. As the purpose of this report is not only to provide an analysis, concrete actions are added to illustrate how to start implementing these recommendations and who can take responsibility.

Resilience and security are since long important issues in the telecoms sector. Telecom operators are required by law to provide a base level of resilience and security. In addition, resilience and cyber-security services can be provided to guarantee high-availability and recovery from disruption. Such services can present a sizable business opportunity.

Resilience means responsiveness and robustness to disruption. Some definitions also include the ability to learn from disruption. Disruption originates in breaches of physical security such as cable cuts and in cybersecurity breaches such as ransomware. **Cybersecurity concerns confidentiality of information, integrity of information and systems, and availability of networks, systems, and devices**. This report considers both cyber- and physical security though with most emphasis on the cybersecurity.

Telecoms is a fundamental critical infrastructure for all other businesses, governments, and citizens. Telecommunications disruption can have an amplified, systemic impact on other sectors. In turn, the telecom sector is highly dependent upon suppliers of chips, computer systems, software, radio towers, cables, connectors, street cabins, and is critically dependent on the electricity sector.

The outline of this report is as follows: Chapter 2 explains the analysis approach. Chapter 3 analyses current security and resilience in the telecoms ecosystem. Chapter 4 considers the forces that affect security and resilience in this ecosystem. Chapter 5 considers actors and their motivations that try to influence these forces, addressing geopolitical, geoeconomical, and other motivations including response to climate change. Chapter 6 gives policy recommendations. These aim to affect actors and their motivations. The hierarchy of the three perspectives of chapters 3, 4, and 5 is intended to help understanding how policy recommendations ultimately affect the telecoms ecosystem.

***Managing expectations**: this report takes a wider and longer-term perspective, beyond economics and beyond today. Recommendations generally go beyond current policy, even if some actions are recommended to start urgently. This report also calls for further study and impact assessment with stakeholders to resolve current uncertainties that are plentiful. This report does not provide a detailed analysis of applicable legislation, although an overview is given. Neither does it provide a detailed analysis of individual issues, although 'who pays for resilience and security' is addressed in more detail. Security and resilience threats and risks are summarized, with further details in references. Finally, this report is constrained by limited resources and by publicly available, and, in some cases, rather sparse evidence.*

2. Analysis Framework

2.1 Scope and Definitions

2.1.1. Scope

The scope of this report is security and resilience that concerns the actors in the telecoms ecosystem. The **telecoms ecosystem consists of the telecoms sector extended with suppliers, customers, authorities and governments** (Figure 1)[219]. The telecom sector consists of companies providing digital communications products and services including telecom operators as well as the telecom equipment industry. The ecosystem notion is also used in other parts of this overall CERRE Telecom study and by the recent White Paper of the European Commission[220], be it in the latter case only including industrial actors.

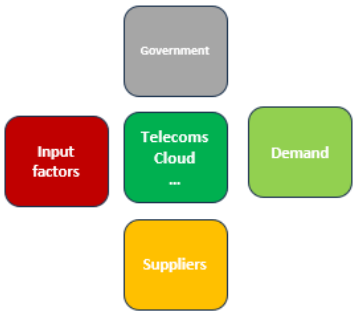


Figure 1 Telecoms ecosystem

In terms of policy interests, this report concerns competitiveness and consumer protection that have always played a role for telecoms policy, as well as economic security and strategic autonomy as related to security and resilience. **Economic security has moved centre stage in the EU** as a consequence of concerns about foreign dependencies in a context of increased tensions with China, Russia's war against Ukraine and the COVID-19 pandemic. The European Commission has over the past year put forward a strategy and several policy actions for economic security[221]. Strategic autonomy in the digital domain (also called digital sovereignty) is the wider set of actions to safeguard sovereignty.

The geographic scope of this report is **mostly the EU as a whole**. At the national level we have to take into account that resilience and security can be very close to national security in which the EU mandate is limited. Namely, Article 4(2) of Treaty on the European Union (TEU), states: "*The Union […] shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State*." Nevertheless, the report discusses how national security can be taken into account at EU level.

2.1.2. Definitions

Resilience is defined in the EU Critical Entities Resilience Directive (CER) as "a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident".[222] *Cybersecurity* is defined by the EU Cybersecurity Act as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber

[219] Modified after (Michael E. Porter, 1990) - factors for national competitive advantage (the diamond model). While Porter's model can be significantly extended such as with industry cluster, innovation and diffusion models, it is still useful as a concise representation of actors and their relations.
[220] (European Commission, 2024b).
[221] (European Commission, 2023, 2024).
[222] (EU Directive on the Resilience of Critical Entities (CER), 2022).

threats".[223] The Network and Information Security (NIS) Directive, the main cyber-law applicable to critical digital infrastructures, refers to this definition. Telecom operators (public electronic communications providers) are critical entities in the CER Directive and essential entities in NIS2[224].

These laws do not use a wider definition of resilience as 'the capacity to deal with change and continue to develop', which originates in social-ecological thinking (Stockholm Resilience Centre, 2020). This wider, pro-innovation view is useful to keep in mind as resilience and cybersecurity are not only about threats and risks but also about opportunities. Resilience and security services can provide important revenue and competitive advantage to companies in the telecoms ecosystem.

Cybersecurity concerns the confidentiality of information, the integrity of information and systems, and the availability of networks, systems, and devices (often called the CIA of cybersecurity). A **common scheme to address cybersecurity risks is Identify – Protect – Detect - Respond – Recover**[225], see Figure 2. This scheme is based on a risk management approach. It does not address the innovation potential of security and resilience.

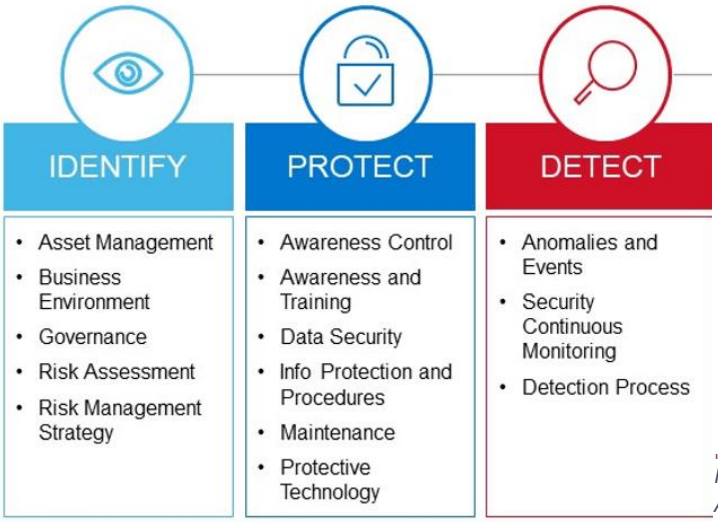


Figure 2 NIST Cybersecurity Framework

Figure 3 Resilience - Economic Security - Strategic Autonomy

Providers are designated as critical or essential because they are perceived as fundamental to the functioning of economy, society, and to some extent democracy. They must be resilient and secure. Since 2017, increasingly thinking has developed that, beyond resilience, also economic security and strategic autonomy are important. *Economic security* is not (yet) defined in the legal sense. Rather, in EU policy, it is stated that it is about dealing with risks of "(1) resilience of supply chains; (2) physical and cyber security of critical infrastructure; (3) technology security and technology leakage; and (4) weaponisation of economic dependencies or economic coercion."[226]

[223] (Cybersecurity Act, Regulation (EU) 2019/881, 2019).
[224] NIST defines cyber resiliency as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.", (Ross et al., 2021).
[225] (Michael Dulavitz (Dell), 2019; NIST National Institute of Standards and Technology, 2018). Diagram based on version 1.1 of the NIST Framework. It is used here as it illustrates in a compact way a number of actions. Recently, NIST issued an update of the framework, see (NIST, 2024).
[226] (European Commission, 2023).

Strategic autonomy can be defined as the capabilities, capacities and control (3C) to decide and act on essential aspects of our economy, society, and democracy[227]. In other words, strategic autonomy is a means to safeguard sovereignty of the state. Strategic autonomy simply said consists of 'what we know', 'how much we can do', and 'how much say we have' in order to safeguard sovereignty[228]. Figure 3 shows how notions relate to each other.

2.2 Three Perspectives

Further to scope and definitions, we analyse resilience and security in telecoms in a three-perspective approach (see Figure 4). The first perspective is an *internal view on the telecom ecosystem* as regards resilience and security (see Figure 1 and central part of Figure 4).

The second perspective focuses on the *external forces that affect the resilience and security* of the telecom ecosystem, as illustrated in the inner ring in Figure 4. The selection of forces corresponds to those generally mentioned in analyses of EU telecoms[229].

The third perspective of the analysis addresses *actors and their motivations*, seeking to influence forces. This corresponds to the outer ring in Figure 4. These can be grouped into geopolitical, geoeconomic, and other geosocial/-environmental/'planet'-related motivations. Actors are EU, countries, companies, civil society, and technology communities. The actors are to be influenced by public policy.

The third perspective in combination with the second and the first helps us to understand how public policy affects actors in their motivations to try to influence the forces that work on security and resilience in the telecoms ecosystem. This enables us to propose recommendations.

[227] Paul Timmers, "Digital Industrial Policy for Europe | CERRE Report" (CERRE, December 12, 2022), https://cerre.eu/publications/digital-industrial-policy-for-europe/; and Paul Timmers, "The Technological Construction of Sovereignty," in *Perspectives on Digital Humanism* (Springer, Cham, 2022), 213–18, https://doi.org/10.1007/978-3-030-86144-5_28.

[228] (Timmers, 2022a). Addressing capabilities, capacities, and control in relation to sovereignty originates from the defence/military domain.

[229] See e.g. (Deloitte, 2023; ETNO, 2024).

Of course, relations between the elements in Figure 4 are more complicated then suggested above. For instance, relations may be two-way with feedback loops and causality is not absolute. Readers are provided here with a set of elements that play a role and may wish to construct relations between elements as they consider fit. This report presents the author's interpretation.

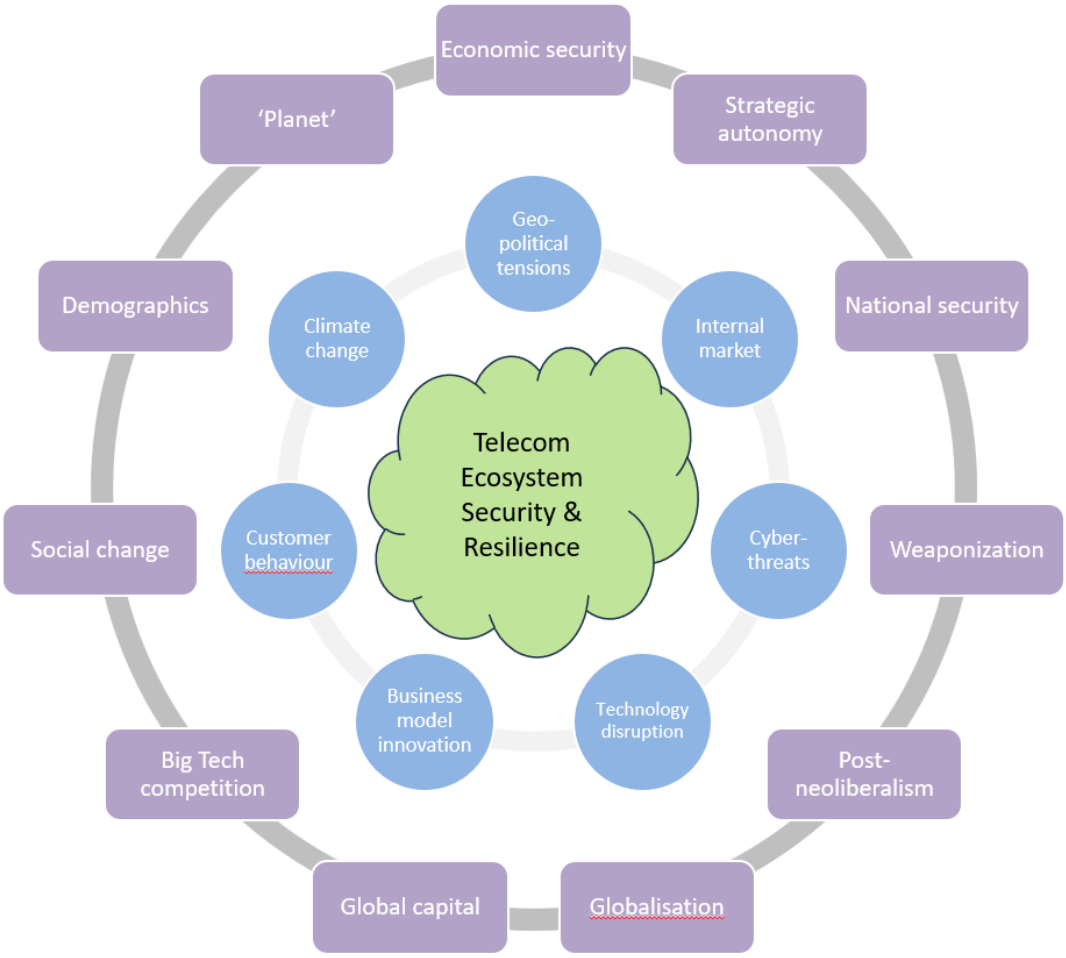


Figure 4 Analysis framework in three perspectives

3. Inside the Telecom Ecosystem

3.1 Structure of the Telecom Ecosystem

The telecom sector is developing towards a telecom *ecosystem*. This is a consequence of the decoupling of Telcos into InfraCos, NetCos and ServCos[230], breaking up previously integrated business (see Figure 5) and emergence of providers of new services. The structure of industry becomes more complex, indeed, rather becoming an ecosystem. In our analysis we also include customers, government, suppliers and providers of so-called factor conditions which are inputs such as capital, and research. In short, we are talking about structural transformation of the telecoms ecosystem (see Figure 1).

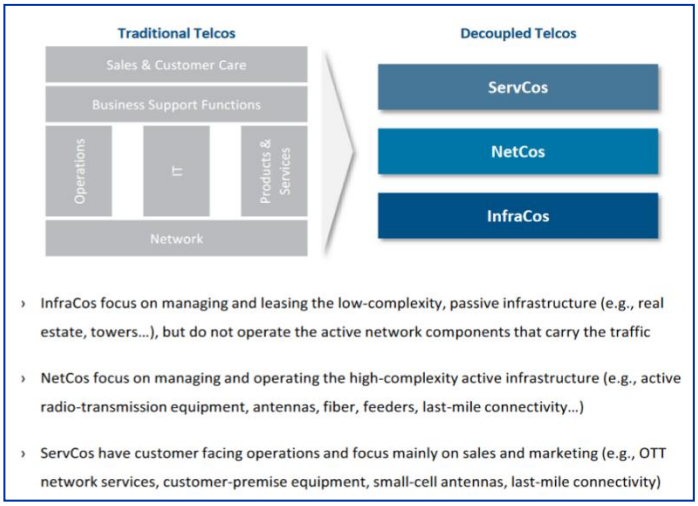


Figure 5 Telecommunication's industry revolution, according to

The dynamics internal to the telecom ecosystem points in the direction of **increased competition**. This can come from specialised providers such as for dark fibre and smart antennas, as well as by cloud and platform providers for both infrastructure and services, and finally by new entrants who provide bespoke and ad-hoc networking services. There will also be increased operation by users of their own networks. All of this is enabled by 5G and 6G technologies and standards.

3.2 Incidents

ENISA[231] summarises **incident reporting in the telecoms sector falling** under the EECC Directive. The latest report, about 2022, shows that over the last 5 years, the number of such reported incidents in the telecoms sector from any origin, physical or cyber, has stabilised between 150 and 170 p.a.[232],[233]. Malicious actions are only 6% of the root cause. ENISA states that 'Comparing incident reporting results over the years, it is fair to conclude that the European telecommunication networks have shown robustness and resilience.'

ENISA found that 18% of telecom incidents relate to physical incidents such as cable cuts (which may be from errant fishing vessels) and arson (which is a physical security issue). Recently, however, there have been an increasing number of cable incidents, from subsea cable rips to copper theft[234], which is starting to become a serious concern.

[230] As (Deloitte, 2023) calls it.
[231] The EU's cybersecurity agency.
[232] (ENISA, 2022).
[233] It is assumed that monitoring requirements are adequate and followed-up ((Ofcom, 2024) expresses the need to review this).
[234] (Georg Serentschy, 2023). In the Red Sea allegedly Houthi attacks have caused several cable cuts. In the Baltic suspicious behaviour by a Chinese ship is linked to cable cuts, (*Making Sense of the Baltic Cable Incidents*, 2023).Telecom operators and large cloud providers have been rerouting traffic in order to keep up bandwidth although latency suffers, see (Mersinoglu &

As regards cybersecurity, telcos experience millions of cyber-attacks daily[235]. Most of these never raise to the level of incidents that have to be reported by law. National authorities receive notification of incidents (both non-cyber and cyber-related), as required by law. For instance, the European Electronic Communications Code EECC (partially superseded by the Network and Information Security NIS2 Directive) and the Critical Entities Resilience CER Directive require the reporting of 'significant incidents'[236]. ENISA also summarizes *cyber*-incidents from public reporting in its annual Cyber Threat Landscape. For cyber-incidents across all sectors, the ENISA Threat Landscape 2023 identified public administration as the most targeted sector (19% of total incidents), followed by targeted individuals (11%), health (8%), digital infrastructure and manufacturing (each 7%), followed by finance, transport, digital service providers and banking/finance (each 6%), see Figure 6[237].

From July 2022- June 2023, the largest share of such incidents consists of ransomware which aims at

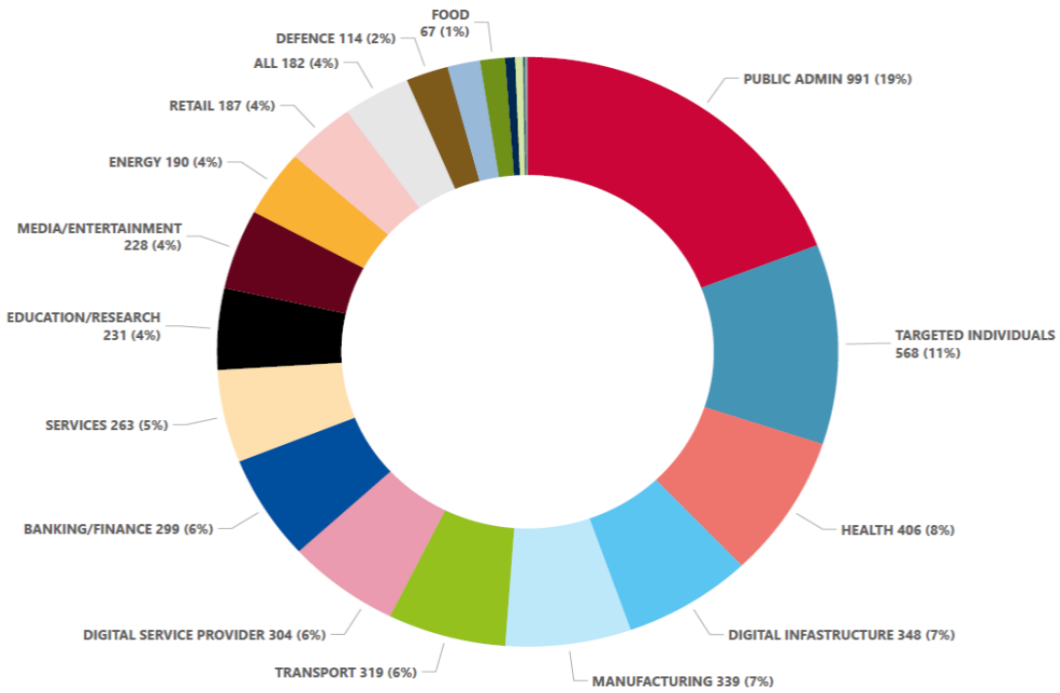


Figure 6 Cyber-incidents by sector, July 2022-June 2023, source: ENISA Threat Landscape 2023

financial or reputational extortion and DDOS attacks which aim to impair availability (Figure 7). Telcos bear the brunt of DDOS attacks[238].

Gross, 2024). Cable cuts happen from time to time. This once again shows that operators and providers have experience managing incidental disruptions.

[235] Deutsche Telekom reports up to 50 million p.d., (Deutsche Telekom AG, 2023).

[236] Although the NIS Cooperation Group provided a taxonomy of incidents, the definition of a significant incident is not quantified nor standardized. The CER and EECC Directives spell out criteria for significant disruptive effect (affected number of users, market share, impact, etc) without quantifying them.

[237] (ENISA, 2023b)

[238] (Zayo, 2023)

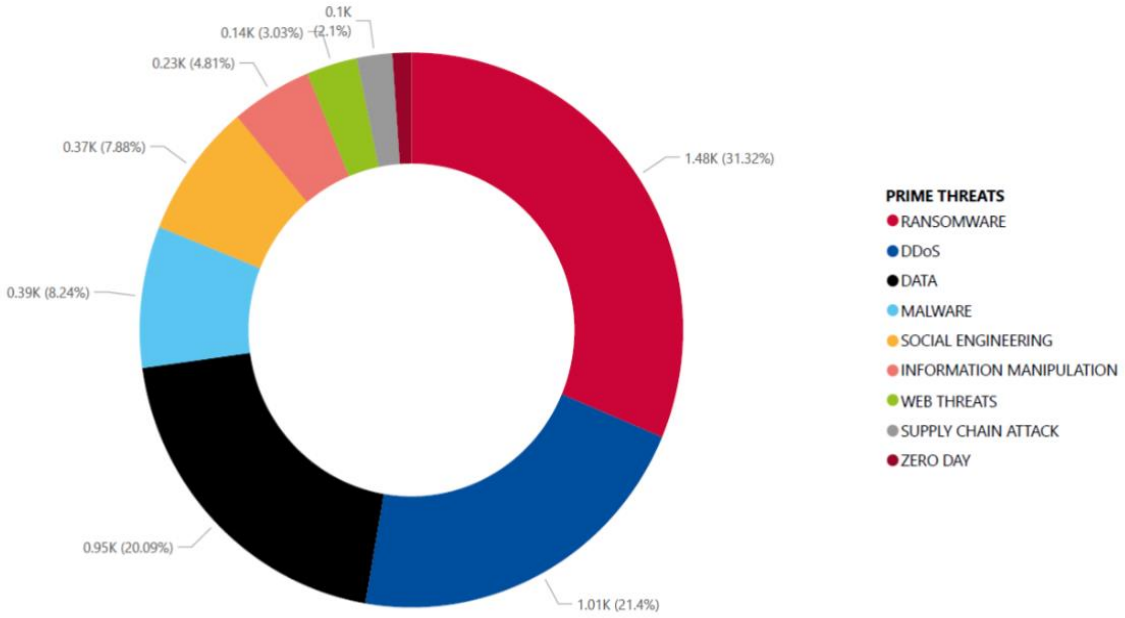


Figure 7 Cyber-incidents by type, July 2022-June 2023 (source: ENISA Threat Landscape 2023)

The European Repository of Cyber Incidents (EuRepoC) which records incidents with a political dimension[239] holds a registry of 35 incidents in EU telecoms amongst 209 critical infrastructure incidents and a total of 2584 incidents, in the period from 2000-January 2024. Of these 35 incidents, 9 concerned disruptions, 21 data theft and the remainder were other types of incidents. For comparison, the transportation sector had 50 incidents, finance 44, energy 32, and defence 26. In state institutions there were 276 incidents, of which 132 in government/ministries (68 data theft, 54 disruptions, and the rest other types) and 84 in public administrations (of which 30 data theft and 42 disruption). Clearly, there are somewhat fewer incidents in telecoms than in several other critical infrastructures and far fewer in telecoms than in state institutions. Moreover, state institutions have experienced relatively more disruption incidents.

As regards impact, incidents reported under the EECC provide number of user hours lost. These added up to over 11,000 million in 2022. Ofcom reports over 100 million hours lost in the UK[240]. Otherwise, there is little systematic information on the extent of damages due to incidents. It is also hard to compare for instance the damage of a leak of customer data with the damage due to unavailability of internet connectivity. According to EuRepoC, state or state-affiliated perpetrators were far more often engaged in data theft than in disruption whereas this was the reverse for non-state actors. Moreover, telecoms cyber-incidents appear to be mostly about data.

Reporting on numbers of incidents and harms only would not do justice to the importance of resilience and security in the telecoms sector. The number of incidents seems relatively low, but there may be several reasons for this. Firstly, the telecom sector is one of the most mature sectors in addressing security and resilience (or business continuity). Legislative requirements have existed since tens of years. Telecom operators know how to raise their defences (but see also footnote 233). Secondly, the telecom sector may well have hidden intrusions by state actors awaiting a moment of exploitation (pre-positioning). Indications that this is the case come from Russian intrusions in Ukraine networks

[239] https://eurepoc.eu/.
[240] (Ofcom, 2024).

before the war started and Chinese intrusion in US networks[241],[242]. In a situation of overt geopolitical conflict, telecoms and in particular mobile communications is likely the first target, as we have seen in Ukraine.

ENISA's 2030 foresight suggests **how incidents may develop in the future**. These can partially be related to the structural transformation of the telecom ecosystem, notably (1) Supply chain compromise of software dependencies: already a priority today, but cyber-crime and malicious actors seem ahead and (2) Cross-border ICT service providers as a single point of failure: in telecoms dependent on the extent of enabling business model innovation by EU internal market/competition policy the numbers referring to Figure 8 below).

Figure 8 Cyber threats in 2030, source: ENISA

The **structural transformations in the telecoms ecosystem can have a positive and negative impact on resilience and security**. A positive impact can come from increased specialisation, stronger security in new architectures and AI-enabled services. The latter may be indispensable in the much more complex digital communications of the future. Growing business interest can be expected for intelligence, analytics, whole-system and dynamic management (e.g., ad-hoc user-driven networks). Negative can be attack surfaces expand as the number of actors and interfaces grow, potentially making the system as a whole more vulnerable[243]. What the balance will be is not known.

The structural transformation also implies that responsibility for resilience and security gets more distributed and with that it risks becoming more diffused and interrelated. From banking and energy, it is known that systemic effects can arise in a system that is composed of a large number of interconnected parts and parties. (OECD, 2023) assesses that the direction is towards a more 'holistic'

[241] Possibly motivated by the wish to acquire the potential for disruption or to engage in less visible forms of data theft such as data exfiltration for espionage or surveillance of opponents rather than data capture by ransomware.
[242] Lessons can be learned from Ukraine ("Russian hackers were inside Ukrainian telecoms giant Kyivstar's system from at least May last year in a cyberattack that should serve as a 'big warning' to the West, Ukraine's cyber spy chief told Reuters.") (Balmforth, 2024). For a US example that came to light in 2023, see Volt Typhoon, (EuRepoC, 2024; Hardcastle, 2024; The Guardian, 2023).
[243] (OECD, 2023; UK NCSC, 2020).

end-to-end approach which addresses and includes all actors, from traditional telcos to cloud and specialised service providers, to the supply chain.

3.3 Current EU Legislation and Policy

An extensive analysis of applicable EU legislation and policy for telecoms resilience and security is not in the scope of this study. Nevertheless, an overview is provided in Table 1. Some observations:

- This is a complex, **extensive set of rules**. (BEREC, 2023) states "[…] operators have just undergone a significant effort to comply with the new (EECC) national security and integrity legislation, therefore it would be useful to have a thorough and comprehensive listing of the additional requirements posed by the NIS2". Several actors express concerns about consistency and coherence, from definitions to applicable rules, and consequently legal certainty[244].
- There is a need to **support the implementation** of the laws. (BEREC, 2023) ask for "training and guidelines from relevant EU institutions on cybersecurity risk management measures and NIS2 additional requirements; consultations, workshops, and industry feedback initiatives […]; support from national competent authorities and ENISA and […] cooperation and information exchange with NRAs on security-related matters, including NIS2."
- **Fragmentation** continues to be a risk as obligations on coordinated risk assessments are limited to ensuring that these are taken into account. There may also be nationally determined obligations such as for legal interception and data retention as well as transposition differences.
- **Inter-sectoral linkages** remain to be further developed, although some work has been done on electricity – telecoms
- In practice, obligations on some foreign dependencies (e.g., extraterritorial subsea cables, foreign ICT supply chains) may not be enforceable.

[244] Amongst others, DT, Ofcom.

Table 1 Relevant law and policy in relation to resilience and security

EU POLICY INSTRUMENT	LINK TO TELECOMS	CONSIDERATIONS
ELECTRONIC COMMUNICATIONS CODE EECC DIRECTIVE	Partially replaced by NIS2, internal market-based	Supporting transition towards NIS2, clarifying national roaming during emergency situations (BEREC)
NETWORK AND INFORMATION SECURITY DIRECTIVE NIS1 2016, NIS2 2022	Internal market-based, telecoms as 'essential entities', cyber risk assessment incl. physical security of ICT systems (effect criterion) e.g., theft, fire, flood, power failures, unauthorised physical access; large-scale EU-wide cyber-crisis cooperation EU-CyCLONe; supply chain obligations are all-hazards approach to mitigate, under risk management, MS may coordinate in this.	Potential risk of fragmented and partial implementation in ICT supply chain security, cf. experience with 5G security, NIS2 states that operators are 'to take into account' risk assessment. Impact on the markets of NIS-2 transpositions across EU, need for guidance and training from EU (BEREC)
CRITICAL ENTITIES RESILIENCE DIRECTIVE CER, 2020	Physical security (non-cyber, but with significant carve-outs for physical security of network and information systems by NIS2). Telecoms are 'critical entities' (the same as essential entities as under NIS2), internal market-based	CER and NIS2 requirements are similar but for some definitions (e.g., significant disruption); telecoms mostly fall under NIS2.
CYBER SECURITY ACT CSA REGULATION, 2019	Establishing cybersecurity certification framework in internal market with certification schemes by EC Implementing Act. Also reinforces ENISA.	Certification may reference contractual clauses for integrated telecom providers with internal and external managed security providers. Assurance level still to be determined (conformity self-assessment, third-party certification).
CYBER RESILIENCE ACT CRA REGULATION, 2024	Cybersecurity of products with digital element, esp. connected products, Regulation internal market-based	Contributes to supply chain certification

		Foreign certification may be difficult if there is geopolitically motivated exclusion of access of inspectors[245].
CYBER SOLIDARITY ACT REGULATION, 2024	European cybersecurity alert system, cyber-reserve with private sector. Managed security services certification is relevant for telecoms (risk mgt, incident handling, penetration testing, security audits, technical consulting).	Most other Acts are based on TFEU Art 114 Internal Market but this Regulation is based on TFEU Art 173 Industry;
E-PRIVACY DIRECTIVE, 2002, 2009	Safeguarding confidentiality of communications	Revision proposed but not adopted; data retention not in scope
ELECTRICITY CYBER SECURITY NETWORK CODE, 2024	Network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows	Delegated Act to Regulation on internal market for energy; closely linked to NIS2 but not identical.
CYBER DEFENSE POLICY, 2022	NATO to enhance dialogue with the telecoms private sector on requirements such as for fall-back.	War in Ukraine brings important lessons for protecting telecom networks, locations services and satellites services.
UN NORMS AND CBMS, ONGOING	Norms of state behaviour and confidence building measures (CBMs such as cyber-capacity building) and possible UN cybercrime treaty (e.g., on lawful access).	Influencing negotiations, where traditional telecoms engagement are far behind some platforms providers Contribute to cyber-capacity building in developing economies

[245] We can learn from the pharma sector as regards supply chain certification. The FT reports that "Pharma groups warn of supply crunch over China spying law - Factory inspectors refuse to visit country over fears they could fall foul of tightened rules",(Johnston et al., 2024).

ECONOMIC SECURITY PACKAGE, 2013, 2014[246]	Packages of measures, some legislative including on FDI controls, IP protection, dual-use research, export controls, tariffs; generally about protecting infrastructure, supply-chain diversification, investment in critical technologies and cooperation with like-minded partners. Identifies key technologies as regards their enabling and transformative nature, risk of civil and military fusion, risk for human rights.	EU economic security action may be directly relevant for telecoms but not covering whole telecom ecosystem: "advanced connectivity, navigation and digital technologies" is one of 10 key technology areas in this policy. Risk assessments have started recently on quantum, AI, advanced semiconductors, biotechnologies.

[246] (European Commission, 2023, 2024c).

3.4 The Business of Security and Resilience

Since many years, business continuity/resilience and security have been part and parcel of business and mind-set in the telecom sector[247]. Business continuity management systems that help organizations to protect and recover from disruptive incidents are supported by international standards such as ISO 22301:2019. Significant business continuity/resilience and (cyber-)security services are provided by telecoms operators and value-added service providers.

(ETNO, 2024) states that "Security revenue is […] rising, albeit with higher initial investments, but its relative proportion of non-connectivity-related spending decreased from 20% in 2018 to 16% in 2022". What is different today compared to the past in resilience and security, is the rise in importance of cybersecurity in combination with other changes indicated in Figure 4. ETNO states that "Cybersecurity is now a fundamental component of enterprise operations and has become integrated into various products and services (though not necessarily just those on offer from network operators). While this limits the necessity for separate security purchases, it does give the added benefit of increasing networks' resilience to cyber-attacks."

This suggests a mixed picture: **to some extent cybersecurity goes into the top line (i.e. increasing telecoms revenues) but to some extent also into the bottom line (i.e. incurred as a cost by telcos) be it that it is then argued to contribute to resilience overall**. It is not transparent from public data how much revenue that first component represents. It appears that telecom operators' revenue in B2B security was 2.6 B€ in 2022 which represents about 13% of total B2B digital providers non-connectivity revenue[248]. See Figure 9 while the Annex gives more details.

(ETNO, 2024)'s statement suggests that the top line for operators' B2B security business is growing be it not at a sensational rate, with a CAGR of 6.99% and with an even somewhat lower projected YoY growth for 2025 and 2026 of 6.37%. This is 2.5-4 percentage points less than the projected growth of the European cybersecurity market[249] and well below the growth of B2B non-connectivity revenues which as a CAGR of over 13%. Assuming that the connectivity cybersecurity market could grow as fast as the general cybersecurity market, this then suggests that both telecom providers absorb themselves a significant part of cyber security costs, about 1/3rd, though they still recover about 2/3rd - with a profit margin- from customers[250]. Therefore, a considerable part of provision of cybersecurity in the connectivity market gets internalised, i.e. is a cost for the operators.

ETNO data show for B2B non-connectivity digital services a CAGR of 13.15% from 2017-2022 while (McKinsey, 2024) reports about telcos in general and not limited to Europe, a 15% CAGR for 2017-2022. For McKinsey these B2B non-connectivity digital services comprise Internet of Things (IoT) solutions; IT services like desktop management and enterprise mobility; cloud-based solutions like infrastructure as a service (IaaS), platforms as a service (PaaS), and software as a service (SaaS); and security solutions designed to detect vulnerabilities or combat fraud). CAGR figures are high compared to the 3% CAGR of core connectivity.

[247] It is not the intention here to give a historic overview, for references see (Herbane, 2010).
[248] Data are based on (ETNO, 2024). Diagram created with Mistral Large as per mid Mach 2024, Mermaid and Draw.io.
[249] (MENAFN, 2024; Statista, 2023).
[250] Back of envelope: 10% growth is the potential, while 7% is realized, that is, 3% profit potential or about one-third is internalized as cost.

McKinsey also observes that enterprises are increasingly planning to move away from telcos for connectivity and adjacent services, towards system integrators and cloud providers. Especially in security they intend to move to cloud providers, more than in almost any other service.

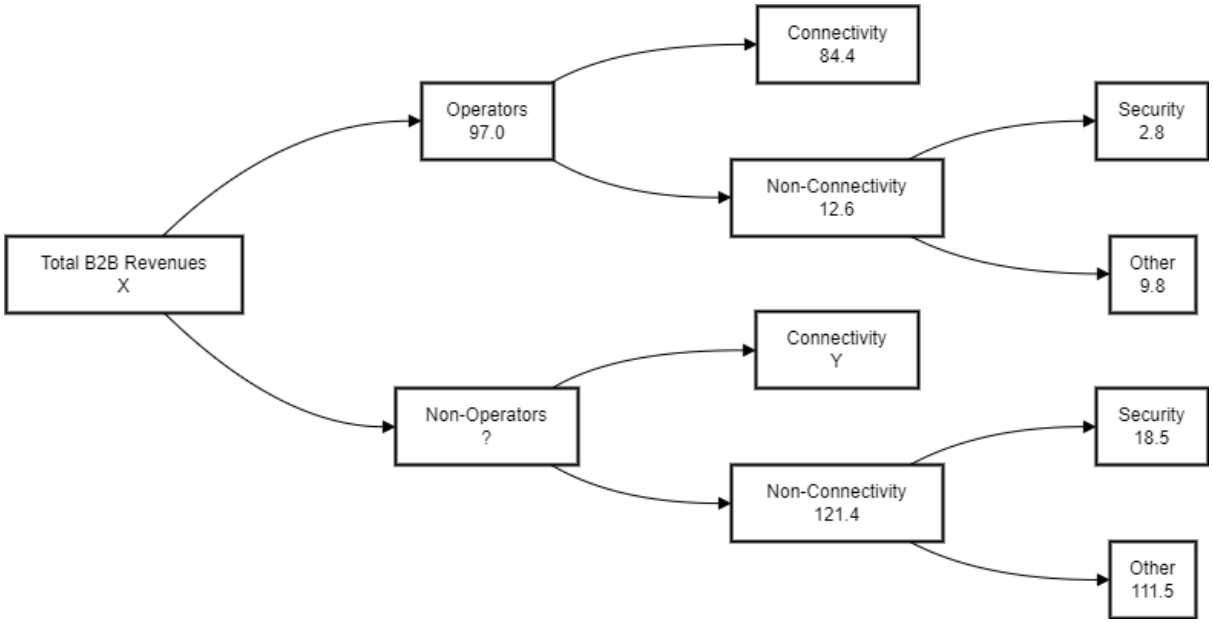


Figure 9 Breakdown of B2B revenues in B€ of digital providers (operators and non-operators) in Europe in 2022

4. Forces affecting the Telecom Ecosystem

The forces considered here are geopolitical tensions, internal market changes, rising and changing cyber threats, technological disruption, business model innovation, changing customer behaviour, and climate change (see Figure 4 above).

4.1 Geopolitical Tensions

The geopolitical temperature is rising due to the war of Russia against Ukraine, the increasing threats of China against Taiwan, the Middle East conflict, rampant mis-/disinformation in a year of critical elections across Asia, the USA and Europe, and the prospect of a Trump re-election[251]. Malicious foreign actors may seize the opportunity to ramp up undermining Europe's resilience and security. Some analysts think that overt war of Russia with EU or NATO countries is a matter of a few years or even less and anticipate a hot conflict over Taiwan by 2027. Western intelligence services believe that a hidden war is already going on[252] and that we are living in a situation of 'unpeace'[253] which will become even more severe over the coming decade. The telecom ecosystem will be a prime target in overt conflict, as seen in Ukraine.

On the one hand the telecom sector appears reasonably well-prepared today, as argued above. On the other hand, challenges to resilience and security will likely increase given indications of hidden infiltration in telecoms systems and increase in vulnerabilities due to the ongoing structural transformation of the telecoms ecosystem. Answering how geopolitical tensions will develop over the coming years amounts to crystal ball gazing. However, one serious possibility is that we will find ourselves after 2024 in a world in which Putin, Trump and Xi have 'won'.

4.2 Internal Market Development

Internal market-based legislation is significantly conditioning the telecom ecosystem. Concerns have been raised from several economic sectors about persistent fragmentation between EU Member States, despite the harmonising effect that Internal Market legislation was intended to have; and stifling impact on innovation due to the complexity and burden to comply with Internal Market legislation. Recently, ways have been suggested to reinvigorate the Single Market[254] including the important report by Enrico Letta[255].

Navigating the large amount of harmonised legislation, let alone navigating fragmentation, is a challenge. In cybersecurity and resilience many laws have been adopted in the past few years. Their sheer volume can be overwhelming even if most experts agree that the laws are necessary. When

[251] (Allison, 2024); (Ivo Daalder, 2024).
[252] (Rathbone et al., 2024).
[253] Level of conflict below overt war but cumulatively as damaging as conventional war (Kello, 2017), (Christian-Marc Liflander, 2024).
[254] (15 EU Member States, 2024; Bruegel, 2023; Reuters, 2023).
[255] (Enrico Letta', 2024).

Internal Market legislation is complex and, worse, fragmented, the result may less security and resilience and increased cost.

In security and resilience, the close relation to national security causes an additional of fragmentation, which is hard to overcome at EU level given the aforementioned Article 4(2) of the Treaty on European Union. The EU has very limited mandate – at has no formal 'competence'- as regards national security, and its hands can be tied.

An illustrative case is **5G security**[256]. Operators had made their network equipment investments based on commercial and technology considerations, and their choices reflected national or legal requirements in force at the time. Yet governments started to worry after these choices had been made as regards the security of 5G. This created a complex and commercially painful situation for operators[257].

The worries notably concerned protection of sensitive information and resilience of the core of government, in other words, this was really about national security. Yet, and remarkable given EU limits in national security, Member States joined up with the EC to develop an EU-level 5G Security Recommendation. In 2019 the European Commission issued this Recommendation to perform technical and non-technical risk assessments on telecoms networks. The Recommendation could not be more than soft law because of the mandate limitations. It was left to the discretion of individual Member State to impose or not a swap-out of equipment from so-called high-risk supplier or high-risk vendors (HRV) on its telecom operators.

The result is a fragmented landscape in the EU with differences in obligation, timing, requirements for core vs access network, etc. Several EU countries but not all of them have swapped out Chinese equipment. This remains a great concern for the European Commission[258]. The problem may repeat itself with fragmentation in dealing with ICT supply chain security in general which, with the extended telecom ecosystem, involves ever more companies, facilities, and services.

4.3 Business Model Innovation

Business model innovation will be enabled by the structural transformation of the telecom ecosystem and is also affected by technological disruption and even by geopolitics. Possible features of business model innovation suggested by literature and positive for future telecoms resilience and security are[259] business models that extend to the whole ecosystem, trustworthiness-based business models including attack resilience, ethical automation/AI, service-centric / 'x-as-a-service' business models[260], and business models that contribute to strategic autonomy and sovereignty.

[256] Very briefly, about in 2018 the US government started to exert pressure on its allies to remove telecoms equipment from Huawei and ZTE because of national security concerns. 5G had not been designed or 'architected' by industry and researchers such that core of government communications could sufficiently be guaranteed to be secure. Governments in the West brought this up at a rather late stage, when 5G was already being rolled out. Governments largely left 5G architecture and 5G standardization, including 5G security, to industry. Governments need to be at the table for a degree of oversight to safeguard their core interests without, however, getting into technical specifications, see (Timmers, 2020a).
[257] See also (UK NCSC, 2020).
[258] Commissioner Breton urged Member States follow up on the 5G Recommendation i.e. ban Huawei and ZTE from telecom networks, (Thierry Breton, 2023a).
[259] (Ahokangas et al., 2024; Timmers & Serentschy, 2024).
[260] Which will, unfortunately, also include cybercrime-as-a-service.

This suggests new opportunities and innovation for resilience-as-a-service and security-as-a-service, yet also new threats and vulnerabilities. Business model innovation may suffer due to security constraints when geo-politics gets the upper hand and companies, capital, and civil society get drawn into geopolitical rivalry and conflict[261].

4.4 Changing Customer Behaviour

Customer behaviour is changing in several ways, of which we want to mention two important ones: **working more remotely and consuming much more data**[262]. Both affect resilience and security. On the one hand they increase the attack surface and the number of high-value assets. On the other hand, they create opportunities for services that guarantee availability, business continuity, and cyber-protection. New actors will also enter the telecom ecosystem such as remote-work platforms and data intermediaries. This suggests that both threats and opportunities for resilience and security will grow, though their balance is unclear at this stage. The willingness of customers to pay for security cannot be taken for granted – as we can also see from consumer ICT - and is addressed in the section 0.

4.5 Technological Disruption

Technology can be and is constructed in a context of governance such as law, economic and national security requirements, ethical guidance, standards, private tech alliances, intergovernmental collaborations, etc. Governance can steer or constrain the shape of technology and conversely, the shape of technology affects governance possibilities. An illustration of governance seeking to shape technology is the trans-Atlantic collaboration on next-generation networks – a form of governance – which sets out to "develop a reference framework for AI in 6G that will pave the way towards global validation, adoption, and standardisation of AI approaches. This framework will enable decentralised AI-based network controls across network domains and physical layers"[263]. Conversely, telecoms security as a technology can trigger new governance (cf., the EU 5G Security Recommendation).

Mobile devices and IoT have massively expanded the attack surface to the extent that cyber-crime has become a whole-of-society concern. At the same time networks become smarter with AI and get smarter architectural design that allows to better compartmentalize security, contain incidents, and provide new services such as timely alerts on cyber-crime attempts. Multi-network 5G and 6G can provide more fall-back options for network failure (e.g., LEO satellite or mesh networks taking over from terrestrial communications). At the same time, ground-based and inertial location services must be also developed as satellite-based GPS signals get increasingly jammed and spoofed. In summary, resilience and security can greatly improve but also deteriorate with technological change.

4.6 Rising and Changing Cyber Threats

Cyber threats are widely expected to both increase and to change in nature. As analysed before, some are related to the structural changes in the telecoms ecosystem. These bring more actors into play – including less experienced ones, lead to a larger number of interfaces, distribute and possibly diffuse responsibility across a larger number of actors and this increase attack surface. At the same time, better architectures, more attention to resilience-by-design and security-by-design,

[261] (Farrell & Newman, 2023) make a strong case that history tells that this is bound to happen.
[262] (Deloitte, 2023; McKinsey, 2023).
[263] (6G-XCEL, 2023).

compartmentalization, specialisation and new security service providers, redundancy and fall-back may all increase resilience and security.

Two more threats were raised by executives at the WEF Davos 2024, which ranked cyber *insecurity* in place four of global risks: 1) talking about the situation in different countries, executives worried about the increasing cyber inequity between those countries and their companies that are cyber-resilient and those that are not. This in turn adds to global economic divides, which is a systemic threat in the age of interdependence 2) the arrival of quantum computing which would be able to break the encryption of today. Experts urge to put in place quantum preparedness now[264].

4.7 Climate Change, Energy-Telecoms Dependency

Environmental factors, generally related to lead to climate change, are increasingly the cause of network failures and disruptions. Climate change is leading to an increase in "natural" disasters (forest fires, floods, landslides) and earthquakes and volcanic eruptions, which can lead to massive outages. Communications infrastructure by its nature can be vulnerable to certain types of weather if buried underground (therefore vulnerable to flood and water ingress); uses overhead cables (which are vulnerable to wind and falling vegetation); or located in high and exposed sites (subject to severe wind, rain and cold conditions)[265]. Around 800 million people live in areas that are constantly threatened by such outages.

This draws in particular attention to the two-way **interdependency of the electricity sector and the telecom sector**. In energy systems, and ever more so in smart energy networks that are necessary to achieve climate-goals and for the sustainable energy transition, electronic communications are indispensable. Conversely, electronic communications networks and in particular mobile networks are critically dependent on resilient electricity supply. Battery and other backup systems for access networks (such as mobile base stations) are not capable of covering more than a few hours of outage (if present at all, see (BEREC, 2022; Ofcom, 2024)).

While addressing this has already since years been in the picture, recently the situation has aggravated, as the impact of climate change e.g. floods has become more severe and looks like to become even more serious, and geopolitically or otherwise politically motivated disruptions in energy and telecoms through sabotage and cyber-attacks are both in the rise and also anticipated to become more severe.

Related are considerations on the impact of ICT on EU sustainability goals[266]. Sustainability goals may impact technological architecture as well as selection of suppliers. This may have both a positive and negative impact on resilience and security.

[264] Some express the need for it as strongly as warning for a 'quantum cybersecurity Armageddon', see (Akshay Joshi, 2024).
[265] (Frontier Economics, 2022), (RegCom, 2022).
[266] See separate chapter in this report by Ilsa Godlovitch.

5. Actors and Motivations

This chapter identifies actors and their geopolitical, geoeconomic, and other motivations that seek to influence the forces mentioned in the previous section.

5.1 Geopolitics

Economic security, strategic autonomy

The **EU is responding to geopolitical tensions by strengthening economic security, and more broadly, by pursuing (open) strategic autonomy**. The goal is to strengthen capabilities, capacities and control and thereby strengthen resilience, build the foundations for future economic strengths - knowledge, jobs, and innovation in the EU-, and safeguard EU democracy and social life.

Insightful in this respect is a geopolitical motivation by European Commissioner Breton for the future Digital Networks Act (DNA): "In the current interconnected world, with rising geopolitical tensions, we need to ensure full control over our decision-making processes in strategic sectors, such as connectivity, and avoid harmful external interference in our EU connectivity infrastructure." He added suggestions for areas to act: "The EU has come a long way in securing 5G networks, which are critical infrastructures in their own right. But there are important loopholes when it comes to securing our network infrastructure in the area of spectrum as well as subsea cables and their (onshore) cable management systems."[267]

Weaponisation

However, acting at EU level has to be 'geopolitically aware', that is, the EU must take into account that adversary geopolitical powers may undermine telecoms resilience and security either directly as a state or through state-affiliated actors. This is a form of weaponisation of telecoms systems.

Weaponisation can take many forms. For instance, the internet can be and has been weaponized for surveillance (Farrell & Newman, 2019). Weaponisation relates to technological change. For instance, for the case of AI, highly capable state threat actors are: "Best placed to harness AI's potential in advanced cyber operations against networks, for example use in advanced malware generation" (NCSC UK, 2024). Threat actors will use AI to identify highly-value telecoms assets, from data to people. Assets such as valuable data and devices will likely be ever more present in the future telecom ecosystem. AI will also be used to develop and rapidly modify malware. AI-assisted response will become indispensable (TNO, 2024), even if this raises serious unresolved legal and political accountability questions (Timmers, 2019a).

International relations theory gives **three ways to counter weaponisation**, namely, defence, deterrence, and de-escalation:

I) Defence means recognising risks and taking preventative measures to make it harder for an attacker to succeed. This requires understanding of vulnerabilities and threats, and knowing which assets

[267] (Thierry Breton, 2023b), (ENISA, 2023a).

require strengthened resilience and security. A recent case are subsea cables. Following worrying disruptions, the EU recommended actions[268] that comprise mapping subsea infrastructure, monitoring, threat and vulnerability information sharing, resilience and security assessment, stress testing, increasing redundancy, increasing repair capacity, investment support for Cable Projects of European Interest, and advanced R&D such as into (quantum) sensors and autonomous subsea equipment, as well as collaboration with NATO.[269] Many of these proposals are still to be put into action and are voluntary, though common risk assessment is an implementation of NIS2 and CER legislation. Defensive preparedness is not for free. A cost analysis is in the textbox below.

Another case to consider are legacy system. While there is a generational step every ten years or so (3G – 4G – 5G - …), telecoms systems still often embed older generations. Their vulnerabilities may therefore remain present, waiting for malicious actors to be exploited (vulnerabilities may also be well-known and well-documented, a notorious case being the SS7 vulnerability[270]). However, legacy systems may also provide a fall-back even if less performant and functional, as when newer systems get overwhelmed such as during the terrorist attacks in Brussels or get damaged as in the war against Ukraine. However, this comes with little guarantee for reliability, availability, and coverage. Largely, legacy systems should be considered a security risk as new technology can offer better security and be phased out, sooner rather than later. In the choice of new solutions, the assessment of suppliers needs to be taken into account, without being naïve: even if high-risk suppliers are avoided, solutions of accepted suppliers may well also still have vulnerabilities.

II) Deterrence means making clear that the adversary would lose much by attacking. Deterrence is hard to imagine in the telecoms sector as potential attackers (e.g., China, Russia, Iran, North Korea) are little dependent on European telecoms.

III) De-escalation means making clear to both sides that there are alternatives in which everyone wins. Long-term de-escalation means identifying common interests that would be damaged if any side undermines resilience and security. Short-term de-escalation means putting in place crisis management and communication between parties to avoid escalatory misunderstandings. Several international platforms engage in de-escalation such as the UN Open-Ended Working Group on ICT security.

The Cost of Increasing Defensive Preparedness

Who pays? Increased resilience and security by preparedness can be covered:

1. in the top line, where the opportunity is to offer additional premium B2B services that deliver guaranteed uptime, latency, bandwidth (up to 2/3rd, see section 3.4)
2. in the bottom line, as a cost shouldered by the private actors in the telecom ecosystem, where a reference is the current level of internalisation of security costs (up to 1/3rd, section 3.4)

[268] (European Commission, 2024b), (NIS Cooperation Group, 2024), (European Commission, 2024a), (ENISA, 2023a).
[269] EU-NATO Taskforce on critical infrastructures, (NATO & EU, 2023) and (EU & NATO, 2023).
[270] (Weinberg, 2023).

3. in public funding for preparedness and solidarity, as already suggested in EU cybersecurity policy, such as for joint exercises and co-investment in redundancy and recovery; and possibly shared insurance.

How much? Total expenditures are hard to assess. They can be a few millions for exercises and awareness raising to potentially hundreds of millions for infrastructure redundancy and recovery. The cost of resilience and security has to be compared to the cost of incidents. The cost of the NotPetya cyber-attack has been estimated at over $10 billion.

National security

It was discussed that national security limits the EU mandate. Therefore, critical to influence geopolitical tensions through **EU action will be the motivation of Member States collaborate for the benefit of their own national security**. The positive experiences with the transition from NIS1 to NIS2 which increased joint approaches, the joint development of the 5G Security Recommendation and recent cooperation on subsea cables give some hope that such collaboration is possible. The increase of linkages between civil and military domains with the help of supranational organisations (NATO, EC) may give further impetus. The threat of war preparedness will also focus minds. The argument can be made that a triple win in terms of national sovereignty and EU sovereignty is quite well possible through EU action[271].

Much of the upheaval about telecoms security and national security has been about High Risk Suppliers (or High Risk Vendors). This led to the EU 5G Security Recommendation with technical and non-technical criteria for supplier selection. Its implementation, i.e., swapping out Chinese equipment, is partial only. The topic of controls on or exclusion of foreign vendors is not new. For instance, (Farrell & Newman, 2023) describe its long history both in the USA and in China.

5G security was the harbinger to address risks in **ICT supply chain security** more generally. The same idea was then taken up in the NIS2 Directive, and for the financial sector in the Digital Operational Resilience Act (DORA) as well as for the electricity sector in a recent Cybersecurity Network Code[272]. ICT supply chain security has also become a major theme in trans-Atlantic cooperation (TTC). This got much momentum due to serious incidents in ICT supply chains, notably deep intrusion, allegedly by Russia, into system management tools for network and infrastructure monitoring of US company SolarWinds.

[271] (Timmers, 2020b).
[272] (European Commission, 2024e).

Further supply chain controls will possible come from the EU economic security package as "advanced connectivity, navigation and digital technologies" is one of 10 technology areas in this policy[273] (see diagram below, from (European Commission, 2023)). Internal market requirements on certification can also be applied for ICT supply chain security. Examples come from the Cyber Resilience Act (e.g., for IoT), and the Cyber Security Act (e.g., for cloud).

5.	**ADVANCED CONNECTIVITY, NAVIGATION AND DIGITAL TECHNOLOGIES**	• Secure digital communications and connectivity, such as RAN & Open RAN (Radio Access Network) and 6G • Cyber security technologies incl. cyber-surveillance, security and intrusion systems, digital forensics • Internet of Things and Virtual Reality • Distributed ledger and digital identity technologies • Guidance, navigation and control technologies, including avionics and marine positioning

Figure 10 Advanced connectivity included in 10 technology priorities of EU economic security

5.2 Geoeconomics

The neoliberal ideal of economic globalisation in terms of trade and global free markets of the past decades got heavily criticized by post-neoliberalist as having failed to deliver sufficient and fair benefits for 'people and planet'. Yet, post-neoliberalists do not swing towards protectionism. Rather they make the case for **combining a degree of protection of national economic interest and regionalisation (national or regional rules) with promoting participation in global markets**[274]. Post-neoliberalists may, however, be less interested to push for global standardisation.

Powerful actors such as global corporations including big tech, global entrepreneurs and fluid global capital continue to be strongly motivated for globalisation. At times they may find at their side the more idealistically motivated tech community and proponents of liberalism in international relations (IR-liberalists)[275] who aspire the democratic and inclusion benefits of global interoperability and open standards.

Competition policy authorities take into account that **open standards and interoperability** can help to safeguard the contestability of future markets. This aligns well with the thinking since many years that open standards and interoperability are often necessary to make the internal market function well. The challenge is to achieve strong resilience and security while in parallel promoting open standards and interoperability. Some of the trade-offs between these objectives are in the textbox

[273] (European Commission, 2023).
[274] (Rodrik, 2023) calls this 'doing economic nationalism the right way', pointing to the economic success nationally and in global markets of several Asian countries such as South Korea.
[275] IR-liberalists are here to be contrasted with IR realists and constructivist. Not to be confused with economic liberalism.

below[276],[277], which also describes how some trade-offs may be based on assumptions and can be turned into win-win's (e.g., on investment see J.P. Morgan's (Wise & Loeys, 2023)).

Trade-Offs or Win-Win's: Competition Policy, Market Access Policy, Industrial Policy

Interoperability is desirable to promote competition. Yet it may expand the cyber-attack surface as more internal interfaces get exposed. However, technology can also offer secure-interoperability-by-design. Governments and regulators should take this into account in competition cases and R&D-industrial policy.

Sharing of infrastructure is desirable for economic efficiency, lower consumer prices and competition, yet may weaken resilience if it leads to single points of failure. Redundancy in combination with symmetric open access may have to be considered in the application of (current) competition policy and encouraged by public co-financing.

Open and global competition seems desirable for consumer benefits yet may not guarantee economic security and strategic autonomy. It is criticized for not delivering public goods in security, resilience, privacy, democracy, and climate and even fair competition and innovation. There is some evidence that modern industrial policy and partnerships driven by strategic autonomy may deliver on both accounts, though they also lead to tensions with partners (cf. US IRA). The EU aspires a balanced approach, 'open strategic autonomy', which should enable to steer away from protectionism, realise long-run competitive advantage (investment analysts advise strategic overweight for IT companies in the EU and US, which include telecoms and protect EU sovereignty.

Post-neoliberalists may advocate resilience and security as a public good but may doubt that economic globalisation is very helpful in this regard. Global corporations and global capital, even while giving primacy to commercial KPIs may embrace resilience and security as they see it is necessary for their long-term economic interests. Whether this delivers is questionable. Where disruptive technologies and business innovation are primarily driven by economic interests, resilience and security do not seem guaranteed to appear. Generally, however, all actors will promote resilience and security, though they may have quite different ideas about the shape of solutions (global – regional, open – closed).

Governments are increasingly motivated to play a role in geoeconomics as they have seen how closely this is related to sovereignty and strategic autonomy. This translates into their growing involvement in technology development and standards. For instance, US and EU governments are now more closely involved and early-on in 6G. The US and a number of likeminded countries have agreed principles for R&D towards a 6G that is 'Secure, Open, and Resilient by Design' of which the first principle is 'Trusted Technology that is Protective of National Security'. Other principles rather stress openness and

[276] Some references for open, global competition: (Wise & Loeys, 2023), (Bradford, 2024), (Simon J. Evenett, 2024), (De Nederlandse Bank, 2023), (Juhasz et al., 2023), (Cohen, 2022).
[277] In the USA concerns have been raised that excessive industry consolidation without controls may increase cyber-risks, see (Tett, 2024).

international and even global collaboration. In the current geopolitical climate, the complete set of principles thus has built-in tensions, which makes one wonder about its effectiveness to 'go global'[278].

The geo-economic stance also affects business model innovation, which as shown before can be positive for resilience and security. When globalisation promotes open standards and open access these are likely to stimulate business model innovation. However, excessive concentration of power in a few corporations may stifle business model innovation. The opposite to globalisation - regionalisation - may also be positive for business model innovation, provided regionalised (e.g. EU) industrial policy stimulates innovation and investment. It may be negative, however, if it raises barriers to trade and investment and is disinterested in global open standards. Inadequate implementation of regionalised policies may also be problematic, a case in point being the recent worries about the Internal Market[279].

The motivation for the Digital Networks Act also includes a strong geo-economic rationale. European Commissioner Breton: "The Single Market is a unique springboard for companies to grow and innovate. It gives us the muscle to set our own rules, assert our sovereignty and be a global player." In other words, a geoeconomic stance translates into directions for the future of the internal market. He also added the more traditional economic arguments in favour of a DNA are, namely, "a cutting-edge telecoms infrastructure is a fundamental pillar for growth, innovation, and jobs creation" and to "attract **more – and more private – capital into our telecoms sector".**

The CERRE Global Governance of Digital Ecosystems report spelled out four resilience recommendations[280]: 1) availability of fall-back solutions in case of network failure (i.e. redundancy), 2) pre-approval for resilience of digital infrastructure equipment, 3) coordinated action for subsea cables and 4) resilience to be considered in case application of competition policy. Of these the first one is to be implemented by operators and tracked by authorities; the second one should largely fall under the NIS2 Directive and possibly the Gigabit Infrastructure Act; on the third see subsea cables above. The last recommendation argues the potential for a positive relation between competition policy and resilience but seems not yet to have been applied in actual cases.

The relevance of the recent new market definition for EU competition policy remains to be assessed. This puts a greater emphasis on "non-price parameters for market definition, including innovation, quality, reliable supply and sustainability"[281]. Relevant here may be a greater emphasis on interoperability that increases supplier choice and rapid switchover to fall-back network systems. This also suggest an opening to achieve or increase resilience by "actions taken due to lack of redundancy, which are classified as market failures."[282]

5.3 Other and Cross-cutting

'Planet'

[278] (The White House, 2024).
[279] (Enrico Letta', 2024).
[280] (CERRE (Pascal Lamy, Bruno Liebhaberg et al), 2022), see in particular the chapter by (Marc Bourreau & Richard Feasey, 2022).
[281] (European Commission, 2024d).
[282] As stated by a European regulator, private correspondence Georg Serentschy.

Another motivation that can affect R&D is sustainability of the 'planet'. Sustainability in telecoms as related to the EU sustainability goals is dealt with in another part of the overall CERRE Telecoms study. Two issues can illustrate the relations of sustainability and resilience and security: decommissioning legacy networks and equipment; and redundancy.

Generally, last-generation equipment and networks are both more environmentally friendly and more secure. In this regard, sustainability and security recommendations for migration or full switch-off of legacy equipment can align, although detailed timing recommendations may differ. Theoretically, where equipment would turn out to have unacceptable security risks and needs to be replaced this may be an opportunity to bring in equipment with a lower GHG emissions.

As regards redundancy, it may be more optimal for sustainability to concentrate, streamline and share telecom infrastructure. However, as the Gigabit Infrastructure Act[283] argues, "in specific circumstances, sharing the infrastructure could jeopardise […] network integrity and security". However, that Act also states that refusing to share infrastructure should come with objective and justified reasons.

Electricity - telecoms

The **electricity and the telecoms sector have critical mutual dependencies**, see Figure 11. Disruptions in electricity supply would create outages in telecoms. Battery backup can only provide a remedy for a short duration, if present at all. BEREC shows a mixed scorecard network resilience in case of power failures: rather optimistic for the core network, far less so for access networks, and with lack of clarity about redundancy and fall-back such as national roaming of emergency services. Ofcom likewise reports a mixed picture[284]. ENISA reports that power cuts represent 13% of the root causes of telecoms incidents and led to over 1000 million user hours lost in 2022 with somewhat higher number given by Ofcom[285].

[283] (Council of the European Union, 2024).
[284] (BEREC, 2023; Ofcom, 2024).
[285] (ENISA, 2024; Ofcom, 2024).

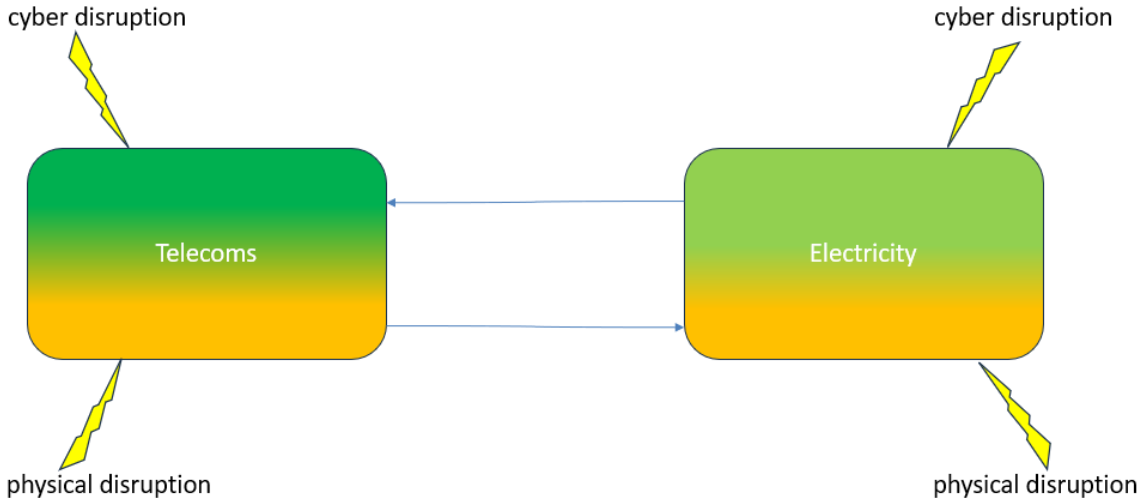


Figure 11 Interdependency of electricity and telecoms

Conversely, disruption in telecoms would cripple operation of electricity networks. Moreover, these get ever more digitized in the move to the smart grids for the energy transition (the 'planet' motivation above). This may again increase the cyber-attack surface. Disruptions can come from geopolitically motivated actors – on the rise; from criminals – on the rise; from human error – struggling to keep up skills; and from natural phenomena such as floods and bad weather – on the rise and ever more severe with climate change. Incidents such as floods may cause both electricity and telecom disruption at (near-)catastrophic scale. (VDE, 2024) gives the example of floods in Ahrtal in Germany in 2021.

This relationship between these two sectors is a vivid illustration of the need for systemic and cross-sectoral risk assessment and risk management. Some of the challenges to address these electricity-telecoms interdependencies are:

- cooperation of authorities from both sectors on risk assessment and incident response;
- differences in definitions such as of incidents, significant disruption, essential entities;
- dealing with at least two reporting channels and sets of monitoring rules;
- bridging IT cybersecurity and OT cybersecurity cultures (OT=Operational Technology);
- differences in cross-border dependencies and practices to deal with cross-border disruption;
- large number of relevant laws;
- sectoral differences in relations to national security, justice, and police;
- coordination in development of supporting standards and guidelines.

Electricity-telecoms is – next to defence-telecoms - the most urgent case for cross-sectoral action on resilience and security. Indeed, increasingly policy-makers and industry call for attention and take action to some extent. (VDE, 2024) provides a set of scenarios including catastrophic ones, (Bundesnetzagentur BNetzA, 2022) spells out a crisis approach with concrete suggestions. The European Commission also starts to address the challenges, see below for the recently adopted cybersecurity network code for cross-border electricity flows. Importantly, the Biden administration

has recognised this too and has recently taken the lead for a major G7 cybersecurity pact to boost the cybersecurity of operational technology in energy systems, which could also become a model for other critical (cross-)sectoral preparedness.

Generalising cross-cutting approaches

With the ongoing structural transformation of the telecom ecosystem, policy for telecoms resilience and security is challenged to deal with:

- a wide variety of actors: large-small, domestic-foreign, private-public, civil-military;
- end-to-end value networks involving a significant number of actors;
- a high level of dynamics and ad-hoc value configurations;
- hybrid situations, requiring combined digital and physical security;
- involving territorial and extraterritorial assets;
- involving domestic and international / cross-border operations;
- geopolitically motivated attacks on the ecosystem.

The telecom ecosystem is not unique in this respect. The same holds for the energy ecosystem[286] but to a lesser degree. It may also hold for future EU satellite and drones' policy. In the context of future revision of cybersecurity legislation (2027), this raises the question if horizontal cybersecurity legislation is sufficient or whether there is a need for additional sectoral cybersecurity soft or hard law.

Sector-specific cyber hard law exists for the financial sector (DORA), which is recognised as a *lex specialis* in NIS2. DORA is a Regulation where NIS2 is a Directive – and can therefore more strongly harmonise. DORA also brings in the specific and extensive governance in the financial sector and banking as well as the notion of systemic risk. DORA has even tighter supply chain ICT security requirements than NIS2.

The electricity sector initially developed a sector-specific cybersecurity Recommendation that complemented NIS1. Recently, however, a Delegated Act to the EU Electricity Regulation was adopted, namely a 'network code' on cybersecurity aspects of cross-border electricity flows[287]. Here too the rationale to not only rely upon NIS2 includes extensive existing and harmonised sector-specific framing, notably the Regulation on the Internal Market for Electricity and its governance, next to the importance of risk preparedness for cross-border flows and systemic effects. Here too supply chain criteria are tightened for the sector: "analyse the cybersecurity risks coming from legacy systems, the cascading effects of cyber-attacks and the real-time nature of systems operating the grid".

It appears then that the pendulum continues to swing between horizontal and vertical legislation but with different timings per sector. Future revision of horizontal cyber-legislation may generalize sector-specific rules such as for supply chain risk handling. At the same time, some arguments above for sector-specific rules may also hold for telecoms such as alignment of sector-specific and horizontal governance, cascading or systemic effects, and risks from legacy systems. In particular, the electricity

[286] Electricity interconnect, subsea pipelines and cables, offshore windfarms, dependency on China for components, etc.
[287] (European Commission, 2024e).

cybersecurity network code provides a reference point for telecoms in terms of cross-border arrangements.

Experience will be built over the coming years with telecom ecosystem-wide application of current horizontal cybersecurity and resilience laws. This will be input for review of horizontal cybersecurity legislation by 2027. Experience over the coming years may show that limited additional vertical telecom resilience and security rules are necessary and desirable. At this moment this is too early to assess, and consequently, a DNA proposal in the short term should not introduce such vertical elements. It also remains to be seen whether Member States are willing to step over their national security reservations and accept stronger harmonisation, i.c., a revised NIS2 as a Regulation.

Recent policy initiatives such as the Economic Security Package, the Critical Raw Materials Act and before that the EU Chips Act show that the EU can mobilise a combination of policy instruments and certainly not only legislative ones but rather a combination of technology research policy, industrial policy, international standardisation, market access policy, competition, trade, and international relations policy. In the EU there is however not yet a corresponding EU telecoms economic security approach.

Integrating policy domains is far from easy, yet this is what geo-economic and geopolitical competition and rivalry may require – this is, for instance, what China does. A holistic policy approach for resilience and security in digital communications has also been proposed by the OECD[288]. More holistic or at least cross-cutting proposals are already advocated by some national authorities and industry groups[289],[290],[291].

Skills and demographics

The **EU has a severe shortage in cybersecurity skills** as confirmed by a recent Eurobarometer[292]. In the telecom sector this is exacerbated by the ageing of the workforce while legacy systems remain in use. There is a clear need to upskills, to retain the knowledge of ageing specialists (what some call the 'COBOL crisis'). This may be alleviated by migrating legacy systems and possibly by deploying AI.

EU policy is limited to coordinating national policies, establishing references for education and training, promoting joint actions at EU level (such as a Cybersecurity Awareness Months) and providing financial support. The EU has no strong Treaty mandate in this regard. Motivation to act on the skills gap and to act jointly has to come from Member States and industry.

Social change

Availability, resilience, affordability are all becoming universal participation conditions. A matter of digital rights[293], which to some extent represents a commercial opportunity but also requires a fresh

[288] (OECD, 2023).
[289] (Bundesnetzagentur BNetzA, 2022; Georg Serentschy, 2024).
[290] NATO committed at its 2016 Warsaw Summit to strive for resilient *civil* communications systems, see (Wolf-Diether Roepke, Hasit Thankey, 2019).
[291] (VDE, 2024).
[292] (European Commission, 2024f).
[293] In fact, a combination of the digital rights in the 'Declaration on digital rights and principles for a human-centred digital transformation' (European Commission, 2022).

look at universal service. Again, this is a little-addressed challenge which is likely to come back and if not dealt with will hit the sector.

Social change includes several other elements such as migration-driven inequality, climate, and conflict; more diverse household and family arrangements, more flexible and ad-hoc work and uncertainty in labour markets due to technological change and (de-)globalisation, the often-quoted erosion of societal trust driven by social media and AI[294], and ageing of the customer population.

With ever-growing dependency on telecoms and value-added services such as e-identification, resilience and security also becoming ever more critical for daily life. At the same time digital skills may not keep up, risking that unprepared and often already vulnerable citizens become victims.

The combined extent of these social changes themselves is uncertain. Their impact on telecoms resilience and security is also hard to predict. Overall, however, they suggest **a need for high levels of flexibility, diversity, and availability of communications**. Likely, mis-and disinformation risks will increase.

[294] Not everyone agrees that this is factually the case. For instance, (Robert D. Atkinson, David Moschella, 2024) argue that this is rather a myth.

6. Policy Recommendations

We are now in a position to put forward recommendations to advance towards the objectives on resilience and security such that these improve both economic/competitiveness and economic security/strategic autonomy. These recommendations target actors and their motivations. Concrete action is added to each recommendation to illustrate how to start implementing them and to encourage the suggested 'action holders' to do so.

The first recommendation recognises that **resilience and security must be tackled by integrated policy**. This does not imply more legislation but rather planning for **mutual reinforcement of policy instruments**. This may seem a rather general recommendation but can be translated into concrete action, even more so in combination with the other recommendations. It may also seem very ambitious, but the analysis shows that a transformational policy change is needed.

Recommendation 1: pro-active engagement of policy makers and industry to develop '**holistic',** (cf. OECD) EU telecoms resilience and security policy that strengthens economic security/strategic autonomy and competitiveness.

Action 1*: EC (CNECT, GROW, DEFIS, COMP), EEAS, ENISA, Member States authorities (as in NIS2, EECC) together with industry to:*

- *Select **priorities** and perform a resilience and security end-to-end analysis of the **wider telecom ecosystem**; such an 'X-Ray' needs to take the comprehensive approach (all parts of the system) and also address technology evolution.*
- *An agenda of priorities comes from the present study, see recommendations below. Further priorities can be based on references in this report such ENISA threat analyses, 5G/6G architecture documents, international and national and industry guidance (OECD, BEREC, NIS Cooperation Group, BundesNetzAgentur, VDE).*
- *Analyse the applicability of **existing policy instruments and legislation** and identify available options and choices; select these such that these are mutually reinforcing*
- *In addition, the **EC to provide Recommendations** to navigate the telecoms resilience and security regulatory landscape and reinforce legal certainty; as well as provide training on the applicable legislation (see BEREC).*

Mostly derived from the geopolitical analysis, more specific recommendations relate to **individual infrastructures**. Action on subsea cables is underway, but we should also consider the security of satellite systems (think of ViaSat ground station cyber-attack), and by implication, need to also have ground-based location services as alternatives to GPS (because of GPS-jamming, GPS-spoofing, satellite vulnerabilities). An issue is also IoT security within the telecom system itself such as for remote monitoring, sensing and control of towers, street cabinets, switches and routers, etc.

Recommendation 2: certain **infrastructures (subsea cables, their landing stations[295] and cable management systems, satellite systems, location services) are a high priority** for policy which may include requirements for redundancy and fall-back networks and enhanced cross-border cooperation in the EU.

Action 2*: similar to the analysis by the EC, ENISA and the NIS Cooperation Group for subsea cables,* ***perform such analysis for the other priority infrastructures****. However, extend the involvement of actors beyond authorities and in line with Recommendation 1 and* ***mobilise the full range of policy instruments*** *where relevant. In particular, develop guidance to apply NIS2 (from October 2024) and CRA (from 2026).*

The next recommendation derives from specific challenges in the geopolitical analysis, in particular preparedness for serious disruption based on understanding of weaponisation intent – physical or cyber - of adversary states. Increasingly, experts and politicians argue that **war-preparedness** is necessary in Europe. This requires comprehensive and consistent preparedness with other critical sectors, notably electricity but also other sectors that depend on telecoms. This is an ambitious recommendation, yet action is indispensable. Action is urgent but will also inform longer-term crisis management in the context of structural transformation of the telecom ecosystem and the forces that affect it such as the changing nature of cyber-threats. It also implements Recommendation 1. It brings added-value in multi-country and cross-border crisis management, while learning from other cases, such as subsea cables and across sectors including electricity-telecoms and civil-military.

Recommendation 3: step up **telecoms cyber- and physical defence**, possibly preparing for war. This must be done coherently with broader policy discussions on defence and deterrence such as with NATO. Associated costs must be recouped in top line, bottom line, and public funding.

Action 3: *industry together with national and EU authorities to urgently perform* ***multi-operator and multi-country / cross-border/ cross-sectoral exercises in disruption and crisis management, fall-back communications, redundancy****, leading to an understanding of bottlenecks and lines of emergency communication. Consider raising public awareness raising, despite this being a delicate matter. Exercises will involve the EU-CyCLONe network, established under NIS2 and EU Integrated Political Crisis Response. Lessons must in particular be drawn as regards the consequences for the wider telecom ecosystem (as NIS2 covers cybersecurity from telecoms to cloud to DNS) and key intersectoral dependencies such as with electricity, finance, health. This must be implemented as a combination of intergovernmental and EU level action. EC and Member States to put forward public funding (the Council has been calling for a Cyber Solidarity Fund).*

Specific points of attention from the analysis are interoperability and redundancy:

Recommendation 4: address trade-offs (between competition policy, market access policy, industrial policy, open strategic autonomy) in **considering requirements for secure interoperability**

[295] (ENISA, 2023a) states "Landing stations are weak points and relatively vulnerable to physical and cybersecurity attacks".

in competition cases as well as in R&D-industrial policy. Also consider in the application of competition policy if **redundancy** with symmetric open access can improve resilience. Consider supporting redundancy by public co-financing.

***Action**: European Commission (DG-COMP) to develop **guidance to assess where interoperability and open access requirements contribute to resilience and security** of telecoms. DG-GROW, DG-RTD and DG-CNECT to provide requirements in Horizon R&D, Digital Europe, Connecting Europe for interoperability and open standards where these objectively contribute to resilience and security. Member States and EC to provide criteria for co-financing of redundancy in Cohesion and NextGenerationEU funding.*

Derived from the geopolitical and geoeconomic analysis, telecoms actors should have a role in defending **global open economy and global collaboration** for stability, safety and security of digital infrastructures. A role that they hardly play today, yet where they can have considerable influence.

Recommendation 5: pro-actively advocate **global collaboration on resilience and security of telecom infrastructures** and promote de-escalation in this context. Promote norms for the protection of transnational communications infrastructures.

***Action**: Industry to engage with EU Member States governments and EEAS to support their work in international forums notably on norms in UN OEWG and to contribute to UN Confidence Building Measures (CBMs) such as cybersecurity capacity building as well as support cyber-diplomacy training and international telecom infrastructure building in the EU's Global Gateway funding initiative.*

A focal point in geopolitical analysis and economic security are international ICT supply chains. The telecom ecosystem is highly dependent on these. It is not clear at this stage what precisely the economic impact is of de-risking. More impact assessment work is needed.

Recommendation 6: critically assess the **impact of different geo-economic strategies** (e.g., globalisation and regionalisation) on telecoms **resilience and security**.

***Action**: industry to urge the EC to **select telecoms ICT supply chains for its economic security risk assessments**. Industry should itself launch a study and seek cooperation with ENISA and the NIS Cooperation Group and use preparatory work such as from JRC to provide its inputs to such risk assessment. Beyond an inventory of critical dependencies and risk classification this should also clarify the pros and cons of strategies such as regionalisation/reshoring vs globalisation/supplier diversification as regards telecom resilience and security. This action may also assess the impact on environmental sustainability of these strategies.*

Derived from the analysis on cross-cutting motivations is:

Recommendation 7: anticipate the 2027 review of horizontal **cybersecurity legislation** aiming that this can address system-wide the telecom ecosystem; while limited vertical cybersecurity measures may be necessary provided **consistency** is strictly maintained, **learning from the experience** of other sectors such as finance and energy; insists on increased harmonization while staying realistic about national security prerogatives.

***Action**: industry across the **telecoms ecosystem should collaborate**, if needed in a separate taskforce, to systematically follow the implementation of NIS2 and other horizontal cybersecurity legislation, as well as EECC, and cooperate with counterparts in the electricity and financial/banking sectors to compare experiences; the outcome is a reasoned opinion on future horizontal cybersecurity and resilience legislation. Combined with the guidance on current legislation (action from Recommendation 1) this can include simplification of legislation.*

Finally, legacy decommissioning is an important theme in the Sustainability Report. In complement to that report:

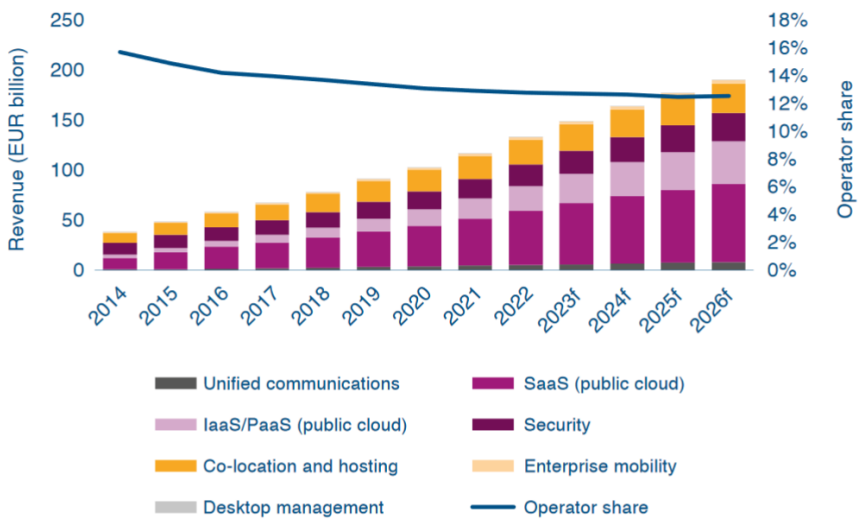
Recommendation 8: policies to **decommission legacy equipment** and networks should also be motivated by security concerns. Nevertheless, if legacy is kept in place for reasons of resilience, guarantees should be provided for reliability, availability, and coverage.

The report also contains some observations on social change as well as on the workforce notably as regards skills gap which may be aggravated by having an ageing workforce that will start to retire while legacy maintenance must be continued. These observations are not translated into specific requirements.

Annex: B2B Security Business

	2022 revenues (€B)	
B2B, all digital providers, Europe	?	
B2B, connectivity, all digital providers, Europe	?	
B2B non-connectivity, all digital providers, Europe	134.0	(ETNO, 2024) Fig. 2.15
Unified communications	5.4	(ETNO, 2024) Fig. 2.15
SaaS (public cloud)	54.3	(ETNO, 2024) Fig. 2.15
IaaS/Paas (public cloud)	24.7	(ETNO, 2024) Fig. 2.15
Security	21.3	(ETNO, 2024) Fig. 2.15
Co-location and hosting	24.8	(ETNO, 2024) Fig. 2.15
Enterprise mobility	2.6	(ETNO, 2024) Fig. 2.15
Desktop management	0.4	(ETNO, 2024) Fig. 2.15
B2B, operators, Europe	97.0	(ETNO, 2024) Fig 2.9
B2B, connectivity, Europe, operators	84.4	
B2B, non-connectivity, Europe, operators	12.6	13% of total, (ETNO, 2024) Fig. 2.15
B2B, non-operators, Europe	?	
B2B, connectivity, non-operators, Europe	?	
B2B, non-connectivity, non-operators, Europe	121.4	
B2B, security, operators, Europe	2.8	assume 13% to security
B2B, security, non-operators, Europe	18.5	
B2B, non-security, operators, Europe	9.8	
B2B, non-security, non-operators, Europe	111.5	

FIG 2.15 : ***Non-connectivity-related B2B services revenue and operators' market share, plus a data table for non-connectivity-related B2B services revenue, Europe, 2014–2026f***



References

15 EU Member States. (2024). Non-paper of Croatia, Czechia, Denmark, Estonia, Finland, Ireland, Latvia, Lithuania, Malta, The Netherlands, Poland, Portugal, Slovakia, Slovenia and Sweden on a new horizontal Single Market Strategy. https://tem.fi/documents/1410877/196402993/15.1.2024+Non-paper+on+a+new+horizontal+Single+Market.pdf/821f6416-9b72-5a77-c203-3e07efb73ed9/15.1.2024+Non-paper+on+a+new+horizontal+Single+Market.pdf?t=1705329103829

Ahokangas, P., Aagaard, A., Atkova, I., Yrjölä, S., & Matinmikko-Blue, M. (2024). Business Models in 5G/6G Mobile Communications. In P. Ahokangas & A. Aagaard (Eds.), The Changing World of Mobile Communications: 5G, 6G and the Future of Digital Services (pp. 137–165). Springer International Publishing.

Akshay Joshi. (2024, January 25). Reflections on Davos 2024: The state of cybersecurity. World Economic Forum. https://www.weforum.org/agenda/2024/01/reflections-on-davos-2024-the-state-of-cybersecurity/

Allison, G. (2024, January 16). Trump Is Already Reshaping Geopolitics. Foreign Affairs. https://www.foreignaffairs.com/united-states/trump-already-reshaping-geopolitics?utm_medium=newsletters&utm_source=twofa&utm_campaign=How%20the%20War%20in%20Gaza%20Revived%20the%20Axis%20of%20Resistance&utm_content=20240119&utm_term=FA%20This%20Week%20-%20112017

Balmforth, T. (2024, January 5). Exclusive: Russian hackers were inside Ukraine telecoms giant for months. Reuters. https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/

BEREC. (2022, June 9). An overview of the BEREC work on the national resilience of network operations. https://www.berec.europa.eu/en/document-categories/berec/reports/an-overview-of-the-berec-work-on-the-national-resilience-of-network-operations

BEREC. (2023, December 7). BEREC Report on the Current Cybersecurity Challenges and Dependencies in Electronic Communication Networks. https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-current-cybersecurity-challenges-and-dependencies-in-electronic-communication-networks

Bradford, A. (2024). The False Choice Between Digital Regulation and Innovation (SSRN Scholarly Paper 4753107). https://papers.ssrn.com/abstract=4753107

Bruegel. (2023, September 15). Enrico Letta receives a European mandate to think about the future of the internal market. https://institutdelors.eu/wp-content/uploads/2020/11/20230915_Report-Letta-ENG.pdf

Bundesnetzagentur BNetzA. (2022). Re-si-li-enz der Te-le-kom-mu-ni-ka-ti-ons-net-ze (Resilience of telecommunications networks). https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Strategiepapier_Resilienz_eng.pdf?__blob=publicationFile&v=2

Cohen, E. (2022). Souveraineté industrielle: Vers un nouveau modèle productif. Odile Jacob.

Council of the European Union. (2024, February 6). Gigabit infrastructure act: Council and Parliament strike a deal for faster deployment of high-speed networks in the EU. https://www.consilium.europa.eu/en/press/press-releases/2024/02/06/gigabit-infrastructure-act-council-and-parliament-strike-a-deal-for-faster-deployment-of-high-speed-networks-in-the-eu/

Cybersecurity Act, Regulation (EU) 2019/881, REGULATION (EU) 2019/881, 2019 15 (2019). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

De Nederlandse Bank. (2023). Geo-economic fragmentation: Economic and financial stability implications. https://www.dnb.nl/media/5bgikcue/dnb-analyse-geo-economische-fragmentatie_7-dec.pdf

Deloitte. (2023). Future of Electronic Communications Networks in Europe—Fact-Pack. https://etno.eu/downloads/reports/20230922_future%20of%20networks.pdf

Deutsche Telekom AG. (2023). Data protection & data security | 2023 Corporate Responsibility Report—Deutsche Telekom. Deutsche Telekom Corporate Responsibility Bericht 2023. http://www.cr-report.telekom.com/2023/management-facts/economy/data-protection-and-data-security

ENISA. (2022, July 27). Telecom Security Incidents 2021 [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/telecom-security-incidents-2021

ENISA. (2023a, August 31). Undersea cables [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/undersea-cables

ENISA. (2023b, October 19). ENISA Threat Landscape 2023 [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

ENISA. (2024). Telecom Security Incidents 2022 [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/telecom-security-incidents-2022

Enrico Letta'. (2024, April 10). Enrico Letta's Report on the Future of the Single Market—European Commission. https://single-market-economy.ec.europa.eu/news/enrico-lettas-report-future-single-market-2024-04-10_en

ETNO. (2024, January 29). State of Digital Communications 2024. https://etno.eu/news/all-news/8-news/788-state-of-digital-communications-2024-etno.html

EU Directive on the Resilience of Critical Entities (CER), Directive (EU) 2022/2557, EU, L 333/164 Official Journal of the European Union (2022). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557

EU & NATO. (2023, June 29). EU-NATO_Final Assessment Report Digital.pdf. https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf

EuRepoC. (2024, January 31). EuRepoC Cyber Incidents TableView. https://database.eurepoc-dashboard.eu/?cyber_incident=3137

European Commission. (2022). Declaration on European Digital Rights and Principles | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles

European Commission. (2023, June 20). An EU approach to enhance economic security [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3358

European Commission. (2024a). Commission Recommendation on the security and resilience of submarine cable infrastructures | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/library/recommendation-security-and-resilience-submarine-cable-infrastructures

European Commission. (2024b). White Paper - How to master Europe's digital infrastructure needs? | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs

European Commission. (2024c, January 26). New tools to reinforce the EU's economic security—European Commission. https://commission.europa.eu/news/new-tools-reinforce-eus-economic-security-2024-01-24_en

European Commission. (2024d, February 8). Market Definition Notice for competition cases [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6001

European Commission. (2024e, March 11). New network code on cybersecurity for EU electricity sector—European Commission. https://energy.ec.europa.eu/news/new-network-code-cybersecurity-eu-electricity-sector-2024-03-11_en

Farrell, H., & Newman, A. (2023). Underground Empire: How America Weaponized the World Economy. Henry Holt and Co.

Frontier Economics. (2022). Climate Change and its Effect on Network Resilience – A study by Frontier Economics. https://www.comreg.ie/?dlm_download=climate-change-and-its-effect-on-network-resilience-a-study-by-frontier-economics

Georg Serentschy. (2023). Network Resilience and physical attacks on telecommunications infrastructure and mitigation measures in Europe.

Georg Serentschy. (2024). Digital Networks Resilience and Security, Policy Implications and Mitigation Measures—Summary.

Hardcastle, J. L. (2024, January 31). Volt Typhoon's botnet infected 'hundreds' of older routers. https://www.theregister.com/2024/01/31/volt_typhoon_botnet/

Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. Business History, 52(6), 978–1002. https://doi.org/10.1080/00076791.2010.511185

Ivo Daalder. (2024, January 25). What another Trump presidency would mean for NATO. POLITICO. https://www.politico.eu/article/what-another-trump-presidency-would-mean-for-nato/

Johnston, I., Alim, A. N., & Barnes, O. (2024, April 21). Pharma groups warn of supply crunch over China spying law | FT. Financial Times. https://www.ft.com/content/1d52d75f-5b54-4c27-bdd4-65409f64c64a

Juhasz, R., Lane, N., & Rodrik, D. (2023). The New Economics of Industrial Policy. SocArXiv. https://doi.org/10.31235/osf.io/gsyq4

Kello, L. (2017). The virtual weapon and international order.

Making sense of the Baltic cable incidents. (2023, October 25). Brookings. https://www.brookings.edu/articles/making-sense-of-the-baltic-cable-incidents/

Marc Bourreau & Richard Feasey. (2022). Addressing Threats To Digital Infrastructure. In Global Governance For The Digital Ecosystems (pp. 143–179). CERRE.

McKinsey. (2023, October 13). Tech talent in transition: Seven technology trends reshaping telcos | McKinsey. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/tech-talent-in-transition-seven-technology-trends-reshaping-telcos?stcr=A376BCBC1F6F42E48AA77C11DB4112E2&cid=other-eml-alt-mip-mck&hlkid=e4abe58a116b4658b8b4ad9e26691754&hctky=12587447&hdpid=a3607672-7328-4e7e-ba66-35cf9a7a31e8#/

McKinsey. (2024, March 4). The core connectivity opportunity in B2B telecom | McKinsey. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/seizing-the-core-connectivity-opportunity-in-b2b-telecom?cid=other-eml-dre-mip-mck&hlkid=c9d7c4b105fb4f4a89bd048046fa3b08&hctky=12587447&hdpid=19a089f1-aab5-4b50-ba49-dbfceb72509b

MENAFN. (2024, March 11). Europe Cybersecurity Market Report 2024-2032 | Industry Trends, Share, Size, Growth And Opportunities. https://menafn.com/1107960880/Europe-Cybersecurity-Market-Report-2024-2032-Industry-Trends-Share-Size-Growth-And-Opportunities

Mersinoglu, Y. C., & Gross, A. (2024, March 16). Telecoms groups reroute Red Sea internet traffic after Houthi attacks | FT. Financial Times. https://www.ft.com/content/bf17fc55-8624-435b-b7dd-bc662a887ba0

Michael Dulavitz (Dell). (2019, March 28). Strengthen Security of Your Data Center with the NIST Cybersecurity Framework. Dell. https://www.dell.com/en-us/blog/strengthen-security-of-your-data-center-with-the-nist-cybersecurity-framework/

Michael E. Porter. (1990, March 1). The Competitive Advantage of Nations. Harvard Business Review. https://hbr.org/1990/03/the-competitive-advantage-of-nations

NATO & EU. (2023, January 23). NATO and the EU set up taskforce on resilience and critical infrastructure. NATO. https://www.nato.int/cps/en/natohq/news_210611.htm

NIS Cooperation Group. (2024). Report on the cybersecurity and resiliency of the EU communications infrastructures and networks. https://digital-strategy.ec.europa.eu/en/news/eus-latest-assessment-cybersecurity-communications-infrastructure-puts-forward-recommendations

NIST. (2024). NIST Releases Version 2.0 of Landmark Cybersecurity Framework. NIST. https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

NIST National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

OECD. (2023). Enhancing the security of communication infrastructure. OECD. https://doi.org/10.1787/bb608fe5-en

Ofcom. (2024, February 12). Connected Nations 2023. Ofcom. https://www.ofcom.org.uk/research-and-data/multi-sector-research/infrastructure-research/connected-nations-2023

RegCom. (2022, December 13). Climate Change and Communications Networks Resilience. Commission for Communications Regulation. https://www.comreg.ie/climate-change-and-communications-networks-resilience/

Reuters. (2023, September 13). EU head asks Draghi to advise bloc on boosting competitiveness. Reuters. https://www.reuters.com/world/europe/eu-head-asks-draghi-advise-bloc-boosting-competitiveness-2023-09-13/

Robert D. Atkinson, David Moschella. (2024). Technology Fears and Scapegoats: 40 Myths about Privacy, Jobs, AI, and Today's Innovation Economy. https://itif.org/publications/2024/05/26/technology-fears-and-scapegoats/

Rodrik, D. (2023, November 7). Doing Economic Nationalism the Right Way | by Dani Rodrik. Project Syndicate. https://www.project-syndicate.org/commentary/east-asian-model-vindicates-economic-nationalism-by-dani-rodrik-2023-11

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). Developing cyber-resilient systems: A systems security engineering approach (NIST SP 800-160v2r1; p. NIST SP 800-160v2r1). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-160v2r1

Simon J. Evenett. (2024). The Costs Of Geopolitical Rivalry For Business—Ten Lessons For Better Policy Design. World Economic Forum. https://www3.weforum.org/docs/WEF_Evenett_paper_2024.pdf

Statista. (2023, March). Cybersecurity—Europe | Statista Market Forecast. Statista. https://www.statista.com/outlook/tmo/cybersecurity/europe

Stockholm Resilience Centre. (2020, December 12). Resilience dictionary [Text]. https://www.stockholmresilience.org/research/resilience-dictionary.html

Tett, G. (2024, April 18). Companies must rethink how they handle cyber risk. Financial Times. https://www.ft.com/content/bfe01131-1ae0-4df8-bdfe-3447def01053

The Guardian. (2023, May 25). China-backed hackers spying on US critical infrastructure, says Five Eyes. The Guardian. https://www.theguardian.com/us-news/2023/may/24/microsoft-china-hacker-critical-infrastructure-us-guam

The White House. (2024, February 27). Joint Statement Endorsing Principles for 6G: Secure, Open, and Resilient by Design. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/26/joint-statement-endorsing-principles-for-6g-secure-open-and-resilient-by-design/

Thierry Breton. (2023a, June 15). Speech by Breton on the cybersecurity of 5G networks [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/speech_23_3314

Thierry Breton. (2023b, October 10). A 'Digital Networks Act' to redefine the DNA of our telecoms regulation | LinkedIn. https://www.linkedin.com/pulse/digital-networks-act-redefine-dna-our-telecoms-thierry-breton/

Timmers, P. (2020a). There will be no global 6G unless we resolve sovereignty concerns in 5G governance. Nature Electronics 2020 3:1, 3(1), 10–12. https://doi.org/10.1038/s41928-020-0366-3

Timmers, P. (2020b, October 13). When Sovereignty Leads and Cyber Law Follows. https://directionsblog.eu/when-sovereignty-leads-and-cyber-law-follows/

Timmers, P. (2022a). Digital Industrial Policy for Europe | CERRE report. CERRE. https://cerre.eu/publications/digital-industrial-policy-for-europe/

Timmers, P. (2022b). The Technological Construction of Sovereignty. In Perspectives on Digital Humanism (pp. 213–218). Springer, Cham. https://doi.org/10.1007/978-3-030-86144-5_28

Timmers, P., & Serentschy, G. (2024). Sovereignty and 6G. In P. Ahokangas & A. Aagaard (Eds.), The Changing World of Mobile Communications: 5G, 6G and the Future of Digital Services (pp. 253–282). Springer International Publishing. https://doi.org/10.1007/978-3-031-33191-6_10

UK NCSC. (2020). Summary of the NCSC's security analysis for the UK telecoms sector.

VDE. (2024, February 5). Mehr Resilienz für die Strom- und Kommunikationsnetze in Deutschland. https://www.vde.com/resiliente-strom-kom-netze

Wise, A., & Loeys, J. (2023). Industrial policy, deglobalization and strategic asset allocation | J.P.Morgan (Global Long-Term Strategy). https://d1e00ek4ebabms.cloudfront.net/production/uploaded-files/JPM_The_Long_term_Strate_2023-01-27_4318021-91952e6d-55c7-4f46-97ad-3cbc444609c7.pdf

Wolf-Diether Roepke, Hasit Thankey. (2019, February 27). NATO Review - Resilience: The first line of defence. NATO Review. https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html

Zayo. (2023, August 24). DDoS Attacks in H1 2023 Up 200% from 2022 According to New Zayo Data | Press Release | Zayo. https://www.zayo.com/newsroom/ddos-attacks-in-h1-2023-up-200-from-2022-according-to-new-zayo-data/

Zysman, L. T. & J. (2023, November 17). The New Industrial Policy and Its Critics | by Laura Tyson & John Zysman. Project Syndicate. https://www.project-syndicate.org/onpoint/the-case-for-new-industrial-policy-by-laura-tyson-and-john-zysman-2023-11

cerre Centre on Regulation in Europe

SUSTAINABILITY

ILSA GODLOVITCH

1. The Impact of ICT on EU Sustainability Goals

1.1 Europe's Sustainability Goals

Sustainability has been a key focus of the European institutions in recent years. The 2019 Communication on the European Green Deal,[296] and subsequent 2020 Communication,[297] set out a target for the European Union (EU) to achieve climate neutrality by 2050 with an interim target to reduce greenhouse gas (GHG) emissions by at least 55% by 2030 from 1990 levels. In June 2021, the Council and Parliament adopted legislation that enshrines these objectives into Europe's first Climate Law.[298]

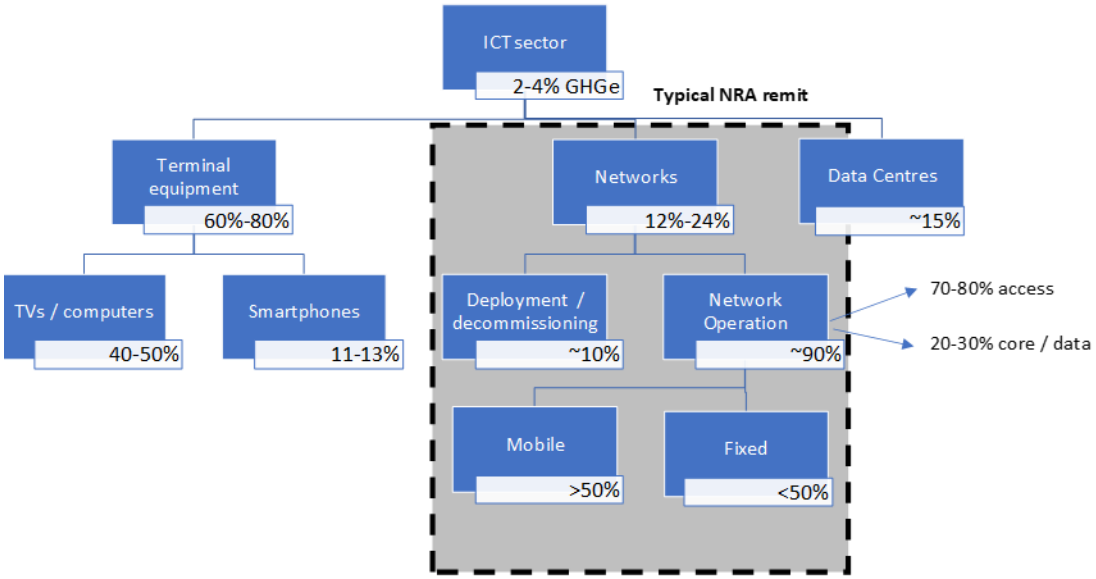
1.2 The Contribution of ICT to Greenhouse Gas Emissions

Available literature[299] suggests that the ICT sector accounts for between 7 and 9% of global electricity consumption[300] and 2-4% of global greenhouse gas (GHG) emissions across its lifecycle[301]. As shown in the following diagram, the majority (between 60-80%)[302] is considered to stem from the production and use of end-user devices, with the highest impacts from large screens (such as TVs and computers). According to most academic literature,[303] electronic communications networks account for between 12-24% of emissions,[304] while data centres are estimated to account for around 15%[305] of the GHG emissions linked to the ICT sector.

Figure 0-1: Breakdown of contributions to GHG emissions within the ICT sector

---

[296] EC (2019) – The European Green Deal, COM(2019) 640 final.
[297] COM(2020) 562 final Stepping up Europe's 2030 climate ambition https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0562.
[298] https://data.consilium.europa.eu/doc/document/PE-27-2021-INIT/en/pdf.
[299] See also figures quoted in the EC 2024 White Paper "How to master Europe's digital infrastructure needs" chapter 2.3.5
[300] Strategic Foresight Report 2022; EU Action Plan on Digitalising the Energy System.
[301] Figures as of 2020. WIK-Consult / Remboll 2022 Study for BEREC on Environmental impact of electronic communications https://www.berec.europa.eu/en/document-categories/berec/reports/external-sustainability-study-on-environmental-impact-of-electronic-communications.
[302] The figures from different sources are not directly comparable, due to differences in the scope of the emissions captured and different interpretations of the boundaries between the different segments constituting the ICT sector.
[303] See section 2.1.
[304] The higher estimates include emissions associated with the manufacturing process. See e.g. Malmodin and Lunden (2018), GeSI (2012), Belkhir and Elmeligi (2018). Andrae (2020) concludes that ECN constitutes around 8% of GHGe excluding manufacturing processes.
[305] As for ECN, a variety of estimates exist regarding the contribution of data centres to GHG emissions. At the higher end, Belkhir and Elmeligi (2018) estimate that data centres account for 41% of ICT's GHG emissions. https://www.sciencedirect.com/science/article/abs/pii/S095965261733233X.



Source: WIK-consult study 2022 for BEREC on the "Environmental Impact of electronic communications"[306]

ICT is not the primary contributor to environmental impacts in Europe or elsewhere, and has been identified as an enabler in reducing greenhouse gas (GHG) emissions in other sectors, for example through smart building, smart energy and transport initiatives.[307] Initiatives have also been put in place to further support the use of digital technologies in achieving reductions in emissions in other sectors.[308]

However, the proportion of emissions coming from ICT could evolve in the coming years, as society becomes increasingly digitised and connectivity is integrated into an increasing range of activities and sectors (and as contributions to GHG emissions from other sources such as housing and transport, decline). While some studies suggest that emissions from the ICT sector will remain largely stable,[309] and that the energy efficiency that will be achieved through digitisation of other sectors will outweigh impacts from the ICT sector itself,[310] others suggest that ICT could account for 14-24% global emissions by 2030/40,[311] presenting an obstacle to achieving Europe's climate neutrality and environmental

[306] https://www.berec.europa.eu/en/document-categories/berec/reports/external-sustainability-study-on-environmental-impact-of-electronic-communications.
[307] A summary of literature is included in WIK (2019) Analysis of the Danish Telecommunication Market in 2030 https://www.wik.org/fileadmin/Studien/2020/Analysis_of_the_Danish_TK_Market_in_2030.pdf.
[308] See for example https://www.greendigitalcoalition.eu/.
[309] See for example Lundén, D. (Telia company); Malmodin, J.; Bergmark, P. (Ericsson Research); Lövehagen, N.: Electricity Consumption and Operational Carbon Emissions of European Telecom Network Operators. Sustainability 2022, 14, 2637.
[310] GeSi (2015) - GeSI Mobile Carbon Impact, IEA (2017) - Digitalization and Energy. Ericsson (https://www.ericsson.com/4ab228/assets/local/about-ericsson/sustainability-and-corporate-responsibility/environment/accelerate-5g-report-27102021.pdf.) claims that connectivity is needed for climate solutions corresponding to approximately 550MtCO2e (equivalent to 15 percent of the EU's total emissions in 2017). Ericsson claims that by 2030, a further 55–170MtCO2e of emissions savings per annum could be enabled by selected 5G specific use cases applied as an illustration of its potential.
[311] Several studies show stable CO2e footprints despite increased bandwidth consumption e.g. Malmodin and Lunden (2018), Ministry of Transport and Communications, Finland (2020) - The ICT sector, climate and the environment. However, future

targets.[312] Beyond climate change, it should also be noted that the ICT sector could also contribute to other environmental impacts including depletion of materials/minerals and water consumption.[313]

The uncertainties regarding the future trajectory of emissions linked to electronic communications is further exacerbated by the lack of reliable and comparable data regarding emissions in the ICT field.[314]

1.3 Sustainability Targets for ICT

In this context, the European Green Deal Communication emphasises that the digital sector itself should be sustainable at its heart,[315] and the Commission's digital strategy[316] underlines the need for the ICT sector to "undergo its own green transformation" and proposes that by 2030, data centres and telecommunications "can and should become climate neutral." The 2023 European Declaration on Digital Rights and Principles for the Digital Decade[317] also includes commitments for Member States to support the development and use of sustainable digital technologies, incentivise sustainable consumer choices and foster sustainable and responsible corporate behaviour throughout the global value chain of digital products and services, promote the development, deployment and active use of digital technologies with a positive impact on the environment and promote sustainability standards and labels for digital products and services.

projections vary with some having a more pessimistic outlook about the future contributions of ICT to global GHG emissions e.g. The Shift Project (2019) – Lean ICT – Towards Digital Sobriety, Andrea and Edler (2015), Belkhir and Elmeligi (2017).

[312] The Shift Project, Lean ICT: achieving digital sobriety (2019) https://theshiftproject.org/wp-content/uploads/2019/03/Lean-ICT-Report_The-Shift-Project_2019.pdf.

[313] BEREC Report on BEREC's role limiting the impact of the digital sector on environment (2022)).

[314]https://www.berec.europa.eu/en/document-categories/berec/reports/external-sustainability-study-on-environmental-impact-of-electronic-communications.

[315]2019 European Green Deal.

[316]EC digital strategy "Shaping Europe's Digital Future" also provides the objective of climate neutrality for digital infrastructures. s.16 Data centres and telecommunications will need to become more energy efficient, reuse waste energy, and use more renewable energy sources. They can and should become climate neutral by 20 https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf.

[317] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001.

2. Mitigating Environmental Impacts from ICT

2.1 The Main Drivers of Environmental Impacts

Environmental impacts linked to ICT include Greenhouse Gas (GHG) emissions, which are linked to energy consumption and may be produced at all stages of the lifecycle. Key factors underlying the trajectory of GHG emissions from ICT include:[318]

- The proliferation of fixed and mobile devices;
- The development of bandwidth-intense applications such as AR / VR and high resolution video as well as the associated devices. The degree to which demand for bandwidth (and thus overall traffic) will increase, which may be linked to the use of bandwidth-intense applications and proliferation of devices (personal and IoT);
- The increasing role of applications involving big data and data processing including AI which require significant computing power and risk increasing energy consumption requirements in data centres;
- The evolution in energy efficiency of devices and networking equipment;
- The source of energy used to produce and power ICT equipment.

Other aspects of environmental impact from ICT include water consumption, loss of biodiversity, and the use of raw materials including rare earths in the production of equipment.[319].

2.2 Measures to Mitigate Environmental Impacts from Devices

As a significant proportion of the environmental impact related to digitisation stems from the production of ICT equipment and end-user devices, measures which support re-use and recycling of equipment and/or components have an important role to play in limiting emissions and the use of raw materials.

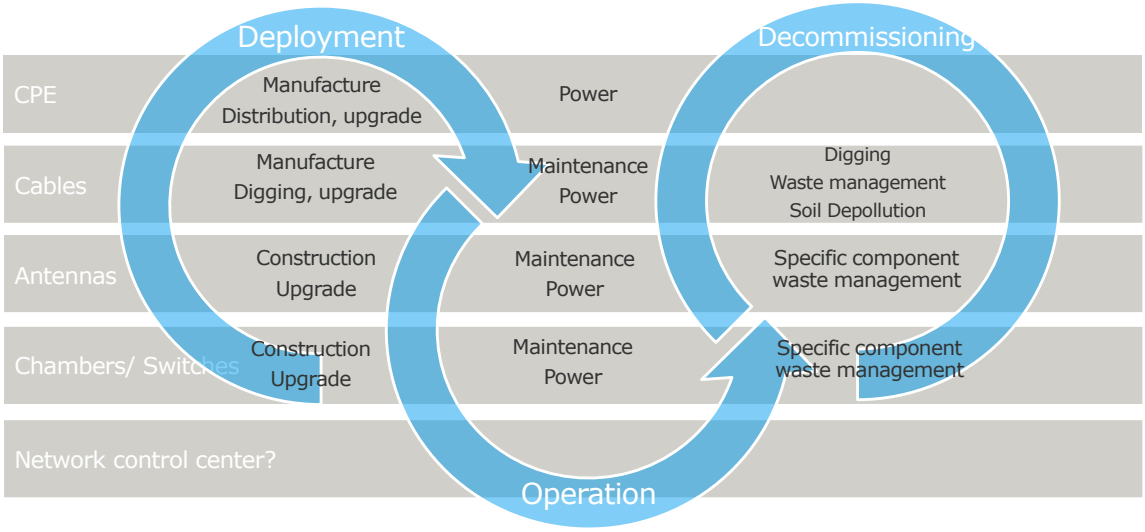
On the supply-side measures could include requirements to factor-in sustainability (such as energy-efficient power-down functions) and reparability in the design of products, while requirements to standardise labelling and provide information about energy consumption in the production and/or operation of products can enable consumers to make more sustainable choices.

[318] https://www.berec.europa.eu/en/document-categories/berec/reports/external-sustainability-study-on-environmental-impact-of-electronic-communications.
[319] See discussion in BoR (22) 93 Assessing BEREC's contribution to limiting the impact of the digital sector on the environment https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-sustainability-assessing-berecs-contribution-to-limiting-the-impact-of-the-digital-sector-on-the-environment.

2.3 Measures to Mitigate Environmental Impacts from Telecom Networks

As regards telecom networks, environmental impacts can be distinguished between those occurring at the deployment phase, the operational phase and the decommissioning phase. An overview of the drivers of environmental impacts at each stage of the lifecycle is shown in the following diagram.

Figure 0-1: A lifecycle overview of the environmental impacts for electronic communications networks



Source: Ramboll and WIK-Consult[320]

2.3.1. The Deployment Phase

For the deployment phase, as literature suggests that most significant environmental impacts stem from laying cables in asphalt, [321] impacts could be reduced by re-using existing civil infrastructure such as ducts and poles, or if that is not possible, engaging in civil works co-ordination or practices such as microtrenching, which involve reduced footprint for digging. [322] Network sharing, at least of passive infrastructure can also reduce the need for parallel construction, which in turn limits associated environmental impacts. This could take the form of wholesale only models or co-investment in a common fibre network, or mast sharing in the case of mobile networks. [323]

[320] https://www.berec.europa.eu/en/document-categories/berec/reports/external-sustainability-study-on-environmental-impact-of-electronic-communications.
[321] Solivan (2015) - Life Cycle Assessment on fiber cable construction methods.
[322] See for example Carbon Smart (2017) - Our digital infrastructure needn't cost the earth.
[323] Kouloumpis et al. (Performance and life cycle assessment of a small scale vertical axis wind turbine, 2020) and Stavridou (A comparative life-cycle analysis of tall onshore steel wind-turbine towers, 2020) both find that foundations are a key source of environmental impacts for wind turbines.

Choices made by operators at the deployment phase can also affect environmental impacts at other stages in the lifecycle or over time. For example, choosing to deploy a more modern technology such as FTTH could help to reduce energy consumption in the operational phase, while opting to construct infrastructure with spare capacity to meet expected future bandwidth needs e.g. larger ducts or deploying point to point networks might involve greater short-term environmental impacts at the deployment phase, but reduce the need for additional construction and/or network upgrades at a later time.

Decisions made by regulators and policy makers can also influence which technologies are deployed and how many sites are required as well as influencing the type of equipment deployed. For example, the choice and amount of frequencies assigned to mobile influences the degree of network densification required to achieve given levels of mobile quality and coverage,[324] while refarming existing spectrum can limit the need for additional radio equipment. Assignment of frequency bands to different technologies e.g. mobile as compared with unlicensed spectrum that can be used to increase capacity on Wi-Fi, could also influence technological choices and thus energy consumption and GHG emissions.

2.3.2. The Operations Phase

In the operations phase the largest environmental impacts are linked to energy use, which may further increase in the context of softwareisation and virtualisation of networks. Against this background, measures which increase the energy efficiency of networks play a key role in limiting the environmental footprint. This includes making use of fixed rather than mobile[325] networks where possible / available, and relying on more energy efficient FTTH networks instead of DOCSIS cable or upgraded copper networks, which consume more energy for a given bandwidth. [326] Sharing of active network equipment including RAN-sharing and measures to facilitate the switch-off legacy fixed and mobile networks to avoid parallel operation of different network generations could also contribute to reductions in energy consumption.[327] Deploying CPE such as set-top boxes with dormant mode and temporary network shutdowns e.g. overnight can also save on energy.[328]

[324] Specifically, higher frequency bands offer additional capacity, but with reduced coverage, thereby requiring additional sites.

[325] Mobile technologies are found to be in general less energy efficient per Gigabit transmitted than fixed. Some studies suggest that 5G is significantly more efficient than earlier generations of mobile technology. For example, Köhn, Gröger and Stobbe (2020) find that 5G networks consume around 5 grams, with 13 grams for 4G and 90 grams CO2e for 3G network per hour of video streaming. However, the overall energy and emissions impacts of 5G, are still uncertain, as studies carried out in Switzerland (https://www.ifi.uzh.ch/en/isr/news/news/5G-study-published.html) and France (https://www.hautconseilclimat.fr/wp-content/uploads/2020/12/rapport-5g_haut-conseil-pour-le-climat.pdf) indicate. While a 5G antenna currently consumes around three times more electricity than a 4G antenna, power-saving features such as sleep mode could narrow the gap to 25% by 2022 https://www.iea.org/reports/data-centres-and-data-transmission-networks.

[326] Studies by Obermann (2020), as well as Aleksic and Lovric (2014) find that fibre-based networks (GPON and point to point) are more energy efficient than FTTC (VDSL2 vectoring, super vectoring) and cable.

[327] In a 2020 study, "Neutral fibre and the European Green Deal", WIK-Consult concluded that a complete migration from the fixed broadband technology mix in the EU to all fibre would reduce emissions by 90% if broadband usage and existing power sources for electricity remained unchanged. https://stokab.se/download/18.15d457b6178eff38ee02ed/1619701526100/Neutral%20fibre%20and%20the%20European%20Green%20Deal%20,%20WIK-Consult.pdf.

[328] https://www.berec.europa.eu/en/document-categories/berec/reports/external-sustainability-study-on-environmental-impact-of-electronic-communications.

Telecom operators can also influence the environmental impact of their services through their choice of energy source. Making use of green energy for the office facilities and operation of telecom networks (including through green procurement) can play an important role, if it does not result in the diversion of green energy from other sectors. This could include self-powering of masts, especially in rural areas, although such solutions also require battery storage, which may have other environmental implications.[329]

2.4 Measures to Mitigate Environmental Impacts from Content and Applications (Including Data Centres)

It is also important to consider the environmental impact of content and services, which can influence energy consumption in content delivery and/or core networks and/or drive energy consumption through more intensive use of consumer devices or computing power, including in data centres.

As regards content, studies suggest[330] that although energy use associated with transmission is only a fraction of in-home energy use,[331] video streaming is associated with greater energy use than broadcast transmission (when transmitting to multiple users). When it comes to devices, the development of high-definition streaming services has increased the attraction of streaming on large screens. However, streaming on larger devices such as a TV consumes considerably more energy than streaming on smaller devices like tablets and laptops.[332] Music as a service applications have popularised the streaming of music. However, streaming a song uses double the battery life compared with playing a downloaded song.[333]

Meanwhile, blockchain has been identified as contributing to driving increased energy consumption due to the need to power the decentralised network of computers. Looking forward, there are concerns that emerging applications based on the "metaverse" (using VR/AR), big data processing and AI in particular[334] could result in increased energy consumption due to the need for increased computational and processing power in data centres[335] alongside performant communication

[329] See for example https://www.vodafone.com/news/planet/self-powered-mobile-masts.

[330] Schien et al. (2020), See IEA Commentary (11.12.2020) by Kamiya, G., https://www.iea.org/commentaries/the-carbon-footprint-of-streaming-video-fact-checking-the-headlines, and the Shift Project (2020), https://theshiftproject.org/wp-content/uploads/2020/06/2020-06_Did-TSP-overestimate-the-carbon-footprint-of-online-video_EN.pdf.

[331] In a study for Ofcom, it was found that: DTT as a distribution method is currently more efficient than IP-delivered content, however most of the energy consumption is within the home rather than in the distribution system – TV sets, viewing devices, and in-home networks account for 90% of the energy used.https://www.ofcom.org.uk/research-and-data/technology/carbon-emissions-of-streaming-and-digital-terrestrial-television.

[332] https://brightly.eco/blog/environmental-impact-streaming.

[333] https://op.europa.eu/en/publication-detail/-/publication/d3b6c0a1-1171-11ee-b12e-01aa75ed71a1 See also https://tech.eu/2023/11/15/the-environmental-impact-of-audio-and-video-streaming/#:~:text=An%20average%20person%20streams%2C%20on,0.57%20billion%20tonnes%20a%20year.

[334] See for example https://www.wsj.com/tech/ai/ai-energy-consumption-fc79d94f , https://www.nytimes.com/2023/10/10/climate/ai-could-soon-need-as-much-electricity-as-an-entire-country.html.

[335] The International Energy Agency (IEA) recently published its report on the electricity market: global data centre electricity consumption could double, in the worst-case scenario, between 2022 and 2026 and this increase is likely to be driven by AI (due to a demand potentially ten times greater in 2026 than in 2022). This growth will mainly depend on the pace of AI deployment and whether efficiency gains are achieved. https://www.iea.org/reports/electricity-2024.

networks, although such applications could also contribute to reduced energy consumption e.g. if they contribute to reductions in the need for travel or supports energy efficiency in other sectors. [336]

Mitigating energy consumption linked to content delivery could include compression techniques, tailoring resolution to match device needs and/or labelling to make typical energy consumption more transparent. Blockchain networks are seeking to transition to more energy-efficient mechanisms, or relying on renewable energy to power their operations.[337] On-site green energy generation as well as locating data centres in cooler climates to make use of natural air cooling have been amongst measures pursued as a means to reduce CO2 emissions in data centres.

2.5 KPIs and Reporting on Environmental Impacts

Measuring progress against sustainability targets requires clear information about emissions and other environmental impacts on an ongoing basis. However, the lack of consistent reporting and the use of different indicators by those who do report on environmental impacts in the electronic communication sector presents an important challenge in this respect.

The French authorities including ARCEP and ADEME, have taken steps to assess the digital environmental footprint[338] and gather data in a consistent manner from telecom operators and other actors including terminal manufacturers and data centre operators.[339]There is not as yet a system to gather such information EU-wide, but this could change with initiatives by BEREC[340] and the EC[341] to contribute to the development of sustainability indicators for telecom networks.

[336] https://www.sciencedirect.com/science/article/abs/pii/S0268401223000014#:~:text=Running%20the%20metaverse%20requires%20a,Green%20Revolution%20Cooling%2C%202022)

[337] https://insideecology.com/2023/04/17/ecological-impact-of-blockchain/

[338] https://en.arcep.fr/news/press-releases/view/n/environment-060323.html

[339] Since 2020, Arcep has started collecting environmental data from the four main telecommunications operators, which led to the publication of the first two editions of the annual survey "Achieving Digital Sustainability" in April 2022, April 2023, presenting, for example, indicators on operator's greenhouse gas emissions, networks energy consumption or mobile phone sales. Arcep's environmental data collection powers were extended by law in December 2021: Arcep is now empowered to collect environmental data from data centre operators, terminal manufacturers, network equipment manufacturers, operating system suppliers, online public communication service providers. Following this extension, Arcep firstly broadened the perimeter of its collection to data centre operators and terminal manufacturers in the third edition of its annual survey published in March 2024 https://en.arcep.fr/news/press-releases/view/n/the-environement-210324.html

[340] The report of BEREC on sustainability indicators for ECN/ECS (2023).

[341] In 2023, the Commission launched a survey to collect input on sustainability indicators. The results are expected to be published soon. See https://joint-research-centre.ec.europa.eu/scientific-activities-z/green-and-sustainable-telecom-networks/sustainability-indicators-telecom-networks_en

3. Implications for the Telecoms Framework

3.1 Legislation Supporting the Sustainability of Electronic Devices

There are a range of existing and forthcoming horizontal initiatives at EU level which seek to promote the sustainability of electronic devices and components as well as data centres.

Examples of legislation include the proposal for a Directive on empowering consumers for the green transition through better protection against unfair practices and better information,[342] as well as the proposed Ecodesign for Sustainable Products Regulation,[343] and proposed Directive on common rules promoting the repair of goods.[344] As electronic elements are being increasingly integrated into devices across many sectors, ranging from cars to household goods, it seems appropriate to handle such issues horizontally on an ongoing basis. Limiting the environmental impact of electronic devices will therefore not be the focus of recommendations in this paper.

Existing Codes of Conduct include the CoC regarding energy efficiency in Data Centres[345] as well as for Broadband Communication Equipment.[346] Although voluntary, the Codes of Conduct provide a mechanism for active engagement and buy-in from the industry, and have involved reporting on key indicators to the JRC.[347] There is plan to complement the existing CoC with a Code of Conduct for the sustainability of telecommunications, which will include some indicators. This is due to be completed by the end of 2025.[348]

3.2 Environmental References in the Current Telecoms Framework

While horizontal measures may be best placed to promote sustainability around the manufacture and re-use of equipment, it is also important to ensure that sectoral legislation, including legislation applying to the electronic communication sector specifically, should at least not run counter to Europe's sustainability objectives and commitments, and should preferably seek to support the achievement of these goals.

The EU Electronic Communications Code (EECC) was adopted in 2018, prior to the conclusion of the European Green Deal. As such, it does not explicitly reference sustainability as an objective, focusing

[342] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directives 2005/29/EC and 2011/83/EU as regards empowering consumers for the green transition through better protection against unfair practices and better information COM/2022/143 final.

[343] https://commission.europa.eu/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/sustainable-products/ecodesign-sustainable-products-regulation_en

[344] https://commission.europa.eu/law/law-topic/consumer-protection-law/consumer-contract-law/rules-promoting-repair-goods_en

[345] European Code of Conduct for Energy Efficiency in Data Centres - European Commission (europa.eu)

[346] Code of Conducts for Broadband Communication Equipment - European Commission (europa.eu)

[347] EU Codes of Conduct for ICT (itu.int)

[348] eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0552

instead on other societal and economic objectives such as those relating to very high-capacity connectivity, competition, consumer welfare and the internal market.

The only mention of the environment in the EECC is in the context of Article 44 which states that:

"Where an operator has exercised the right under national law to install facilities on, over or under public or private property, or has taken advantage of a procedure for the expropriation or use of property, competent authorities may impose co-location and sharing of the network elements and associated facilities installed on that basis, in order to protect the environment, public health, public security or to meet town- and country-planning objectives."

Even here, the reference to the environment is more likely to have been conceived in the context of avoiding disruptive digging procedures or unsightly duplication of infrastructure than necessarily aimed at limiting GHG emissions.

The **Broadband Cost Reduction Directive** of 2014 is focused on measures which promote more efficient deployment practices such as co-ordination of civil works and the re-use of existing physical infrastructure. As such, while also adopted prior to the European Green Deal, it is by nature a pro-environmental measure. However, references to the environment in the BCRD also focus on environmental factors such as pollution and nuisance, or the urban planning rather than the reduction of waste and GHG emissions.[349] The 2023 **draft Gigabit Infrastructure Act**[350] maintains the approach of the current Directive in not explicitly referring to sustainability as implied in the context of the European Green Deal but goes further than the BCRD in supporting physical infrastructure sharing and other sustainable deployment methods, and is thus inherently supportive of the EU's sustainability goals.

The **2023 Broadband Guidelines** introduce references to environmental objectives as well as encouraging Member States to take into account environmental impacts in the context of the award of State Aid. For example:

- Paragraph 8 notes that "One of the essential components of the digital transformation of the Union is the development of secured and performant electronic communications networks that help to make an important contribution to the Union's main environmental objectives. At the same time electronic communications networks themselves will have to become more sustainable, energy, and resource efficient."
- Paragraph 122 notes that: "Member States may consider granting additional priority points for criteria pertaining to the climate and environmental performance of the network, respectively as regards its climate neutrality characteristics, including its carbon footprint, and the impact of the network on the principle components of natural capital, that is to say air, water, land and biodiversity. Member States may also include obligations for the selected bidder to implement proportionate mitigating measures in case the network may negatively impact the environment."

[349] See for example Recitals 13 and 29 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex%3A32014L0061

[350] https://www.consilium.europa.eu/en/press/press-releases/2024/02/06/gigabit-infrastructure-act-council-and-parliament-strike-a-deal-for-faster-deployment-of-high-speed-networks-in-the-eu/

- Paragraph 126 notes that "The use of existing infrastructure is one of the main factors that can contribute to reducing the cost of deployment of a new broadband network and limiting the impact on the environment."

3.3 Tensions with Sustainability Goals

While the Broadband Guidelines, BCRD and draft GIA are consistent with sustainable practices (even if in the case of the BCRD and GIA they do not directly reference them), the EECC includes principles which could (depending on their interpretation and application) run counter to measures that could support reductions in waste and GHG emissions. The following table provides examples of sustainable practices in electronic communications which may create tensions with the objectives that NRAs, BEREC, Member States and the European Commission should meet under the terms of the EECC.

3.3.1. Tensions between the EECC and Sustainability Goals

SUSTAINABLE PRACTICE	TENSION WITH EECC	REFERENCES
Promoting energy efficient technologies such as FTTH	Principle of technology neutrality	Article 3(4)c
Encouraging network and facility sharing including potentially active elements	Promoting efficient infrastructure-based competition	Article 3(2)b
Reducing quality / selective network shutdowns as an energy saving measure	Promoting high quality and availability for connectivity	Article 3(2)d

Regarding **technology neutrality,** the EECC requires in the context of the General objectives in Article 3 that "*The national regulatory and other competent authorities shall, in pursuit of the policy objectives… apply Union law in a technologically neutral fashion, to the extent that this is consistent with the achievement of the objectives*." As the objectives refer to the promotion of VHCN, competition in ECN, the promotion of the internal market and the interests of citizens (with reference to widespread availability and take-up of VHC, choice price and quality, and security of electronic communication networks and services), there does not appear to be scope to favour certain actions (such as network sharing, with the exception of Art 44) or technologies such as FTTH on sustainability grounds.

Regarding **network and facility-sharing**, the requirement that NRAs, other competent authorities, BEREC, the Commission and Member States should promote competition in the provision of electronic communications networks and associated facilities, including efficient infrastructure-based competition, could be interpreted as limiting flexibility for NRAs and others to promote or require network or facility sharing in cases where it may contribute to sustainability goals, but where duplication of facilities or networks is viable, and thus "efficient" from a purely economic perspective.

Meanwhile, the duty as regards the interests of citizens to "enable the maximum benefits in terms of choice, price and **quality** on the basis of effective competition", combined with other measures which seek to reinforce the widespread availability, quality and resilience of electronic communications networks, could run counter to practices whereby coverage and quality might be traded off against energy consumption e.g. in the context of reinforcing mobile coverage in very remote sites, and ensuring availability of high capacities at times of low demand such as nighttime. Spectrum policies which favour usage of higher frequencies and by implication extensive network densification for mobile deployment also risk increasing carbon emissions compared with the use of frequencies at lower bands. More generally, the idea of reducing consumption of materials and bandwidth, could be seen as running counter to the philosophy underlying the EECC (although it is not explicitly stated) that more bandwidth and greater consumption of digital services should be positive for society and the economy and is desired by consumers without regard to its environmental impact.

In addition to areas of tension with sustainable practices, there are also gaps where the EECC does not provide for the necessary powers or measures that would serve to promote sustainability in electronic communication networks and services.

One potential gap identified by BEREC[351] is that the EECC does not explicitly provide for **data gathering powers** regarding energy consumption and environmental impact. This could be important for NRAs seeking to support achievement of the European Green Deal objectives, although may not be necessary if comprehensive EU-wide reporting measures are in place. There are also no specific provisions in the EECC for ECN providers to provide information about energy consumption and emissions in the context of **transparency obligations** for consumers e.g. in contracts and the contract summary. The list of conditions which may be attached to general authorisations make no reference to conditions which may be relevant for sustainability, and while it seems possible to include such conditions in the context of rights of use for radio spectrum, these are not directly referenced and would need to be attached as a commitment which the undertaking made in the framework of the authorisation granting the right of use under Annex 1.D7.

Another potential gap is the lack of an EU-wide aspiration regarding the timeframe for copper switch-off. This contrasts with the clear targets given in the EECC and in the 2022 Digital Decade Policy Programme regarding the need to achieve coverage with Gigabit / VHCN technologies and award spectrum licences for 5G pioneer bands. Another gap is that while Article 81 EECC establishes a process for how NRAs should respond to announcements by SMP operators regarding migration to fibre, this focuses on situations where the incumbent has deployed its own fibre network and wishes to migrate its wholesale and retail customers to its own fibre network. This does not however take into account cases where the incumbent has not deployed fibre, but there is an alternative fibre network available in a given area, a situation which has arisen in many State Aid zones, as well as certain commercial areas. Recommendations have been given in the 2024 Gigabit Recommendation which seek to promote migration in this situation,[352] but are not binding.

[351] BoR (23) 166 suggests that a clearer mandate for NRAs to collect environmental data on ECN/ECS would be welcomed https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-sustainability-indicators-for-electronic-communications-networks-and-services.

[352] The 2024 Gigabit Recommendation notes that equivalent alternative products may be made available by the SMP operator on a regulated or voluntary basis or could be made available by another operator which has deployed VHCN. It also notes that - Switch-off conditions should not be discriminatory. Discrimination could involve differences that are not

In many cases a sustainable approach may dovetail with the economic incentives of commercial operators because sustainability often implies reduced use of materials, construction or energy consumption, which should reduce costs. However, corporate responsibility alone may be insufficient in achieving sustainability goals when there are conflicting interests involved. One example is that sharing passive infrastructure might require the introduction of new processes and security measures e.g. by an energy or sewerage utility or (for broadband providers) impact retail market shares. There can also be tensions when scarce resources are involved such as when different interest groups campaign for the right to use the same spectrum band, and use of that band by the competing parties may influence energy consumption. Switching off legacy networks can also create tensions between network providers and retail or wholesale providers of the networks concerned, as well as consumers and businesses users reliant on legacy equipment. The incentives for owners of legacy copper infrastructure to migrate their customers to fibre may also be limited in areas where they have not yet deployed their own fibre network. Furthermore, while network providers may have incentives to limit cost and energy use in relation to their own networks and equipment, they may have limited incentives to reduce material consumption and encourage the re-use of end-user equipment, in particular when they may be selling such equipment as an adjunct to their telecom services.

Finally, tensions can exist in international standard-setting when stakeholders from different regions have different priorities or obligations (or where Governments might have differing priorities from those of commercial stakeholders). For example, sustainability in the specification of 6G might be an important goal for European policy makers to achieve their environmental objectives, but might be relatively less important for some stakeholders or other regional or national administrations.

justified on the basis of objective criteria concerning the switch-off timeline in areas where the SMP operator has deployed VHCN, compared with areas where another operator has deployed.

4. Conclusions and Recommendations

In conclusion, while clear objectives have been set for the telecom sector to achieve climate neutrality, and recent measures to update the Broadband Guidelines and BCRD (with the GIA) are supportive of this agenda, the EECC lacks any direct reference to or targets in support of Europe's sustainability goals and contains principles which could run counter to achieving them.

If a new telecom framework were adopted today, it would likely include objectives and provisions that do not feature in the EECC. Some initial propositions are shown in the following boxes.

Recommendation 1: Taking Into Account Sustainability Goals Alongside Other Core Objectives Such as Promoting Competition and Consumer Welfare In The Regulatory Framework

A future telecom framework should where appropriate directly favour policies that support sustainability (such as migration to more sustainable technologies, allocation of spectrum bands to specific services, or policies regarding physical infrastructure sharing as are reflected in the GIA). Attention could also be given to policies which impact equipment lifetimes. For example, the abolition of handset subsidies could reduce equipment turnover, while also addressing constraints on switching linked to contractual tie-ins and ongoing payments associated with handsets. For decisions that are taken at national or local level, there should be a requirement for competent authorities to consider sustainability as an explicit objective alongside other objectives regarding competition (including the promotion of efficient infrastructure competition), consumer protection etc. There could also be scope for guidance to NRAs and competent authorities on how to weigh up different objectives in their decision-making through a systematic cost benefit analysis.[353] Other principles in the Framework should also be interpreted with sustainability goals in mind. As regards technology, this means that the telecom framework should, as has already been done in the context of the Broadband Guidelines[354] clarify that while measures taken under the framework should not favour or exclude any particular technology, this does not preclude the ability for competent authorities to take decisions which could impact the choice of technology based on objective factors affecting sustainability such as energy efficiency, and the degree to which the solution minimises construction and use of scarce materials. To this end, the telecom framework should also expressly provide that general authorisations as well as rights of use can include conditions relating to sustainability.

[353] Specifically, it is recognised that some approaches which may be more environmentally sustainable may nonetheless imply higher short- or long-term costs which could raise prices to consumers, or may require trade-offs with infrastructure competition, thereby affecting dynamic competition.

[354] Para 125 Broadband Guidelines note that The technological neutrality principle requires that State intervention must not favour or exclude any particular technology, both in the selection of beneficiaries and in the provision of wholesale access. As different technological solutions exist, the tender should not favour or exclude any particular technology or network platform. Bidders should be entitled to propose the provision of the required services using or combining whatever technology they deem most suitable. This is without prejudice to the possibility for Member States to determine the desired performance, including the energy efficiency of the networks, before the procedure and to grant priority points to the most suitable technological solution or mix of technology solutions based on objective, transparent and non-discriminatory criteria.

Recommendation 2: Establishing Long Term Goals That Focus On The Transition To Low Carbon Future-Proof Fixed and Wireless Connectivity Solutions

An objective of supporting sustainability also aligns with the idea that 'the successor to the Digital Decade targets[355] (which currently refer to Gigabit connectivity up to the network termination point at a fixed location and coverage with wireless networks with performance at least equivalent to 5G) should favour future-proof solutions, which minimise energy consumption in relation to the bandwidth consumed and will not require the repeated replacement or re-engineering of networking equipment and cables. For example, as regards fixed connectivity, rather than establishing specific target bandwidths, and while recognising that it may not be economically feasible or the most sustainable solution in more remote areas, an aspiration to boost the availability of point to point fibre would be consistent with meeting the expanding bandwidth and quality requirements of both consumers and businesses post 2030 while limiting emissions associated with high bandwidths and the need for repeated infrastructure upgrades. . As regards wireless connectivity, the imprecisely defined concept of 5G could be replaced with an aspiration to promote standards for 6G that embeds high standards for sustainability and to achieve leadership in the roll-out of this new technology once standardised.

At the same time, to ensure that efficiencies from new technologies can be realised, an updated framework could establish aspirations regarding migration from legacy technologies to more sustainable modern technologies while maintaining safeguards to ensure that migration occurs in a manner that is efficient, preserves competition and protects consumers and businesses. Achieving full migration and switch-off of legacy technologies is only possible once the future infrastructure is in place. This may require targeted State Aid for sustainable new technologies, in cases where deployment is not commercially viable, and existing State Aid or EU Funds do not meet the shortfall. Attention to copper switch-off conditions may also be needed, to enable and incentivise the rapid migration from copper to fibre once fibre has been deployed (whether by the incumbent or alternative operators). It is relevant to note that in addition to supporting sustainability goals, copper switch-off also facilitates other objectives, serving to boost the business case for fibre investment, and support more secure communications. Switch-off of legacy generations of mobile technology should be encouraged for the same reason.

Recommendation 3: Improving Transparency around Environmental Impacts of Telecoms

Various initiatives are ongoing to improve the availability and consistency of reporting on environmental impacts in telecoms. These include an ITU-T project which would involve regular data collection on sustainability of ICT sector organizations at worldwide level, as well as initiatives by the JRC and the development of a Code of Conduct on Sustainability in telecoms at EU level, which could include indicators. National administrations and regulatory authorities (including telecom regulators as well as environmental agencies) should support initiatives which ensure consistent reporting at a multi-national level, and limit fragmentation and duplication in data gathering exercises.

[355] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022D2481

Alongside corporate reporting, it is also important that consumers and businesses should understand and be able to compare, at least at a high level, the environmental impacts of the services they are purchasing. For example, in addition to information regarding quality such as download and upload speeds, consumer contracts, including contract summaries could usefully contain information about the environmental impact of the service provided, where consistent information is available based on standards and indicators set at EU level. In this context, we note that actions requested from standards bodies[356] include the definition of global KPIs for energy management of fixed and mobile networks, and data networks. If supported by robust methodologies that reflect the full value chain, inclusion of telecom networks in the Taxonomy could also provide a valuable means to allow telecom operators that have deployed networks and services which are energy efficient to label them as such and to use this designation to attract sustainable finance.

While it seems clear that Europe's connectivity targets and regulatory framework should reflect Europe's long-term sustainability goals, applying this principle will require NRAs and/or other competent authorities to make new trade-offs, that will require a deeper understanding of environmental impacts, and involve cost benefit analyses that could be controversial and may require new approaches, to reflect the less tangible and long-term nature of the harms linked to environmental damage.

Finally, it should be noted that adaptations to the connectivity goals or the framework governing electronic communications address only a small aspect of the environmental impacts stemming from ICT. A wider reflection is needed to consider how to avoid increasing impacts from other aspects of ICT as use of services such as AI and AR/VR which require high levels of computing power and/or high bandwidths expand.

[356] https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/ict-environmental-impact-rp2023

cerre Centre on Regulation in Europe

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu

Centre on Regulation in Europe (CERRE)
CERRE Think Tank