EUROPEAN
COMMISSION

Brussels, XXX
[…](2024) XXX draft

WHITE PAPER

"Building Europe's digital infrastructure of tomorrow: towards a Digital Networks Act"

- White paper –

"Building Europe's digital infrastructure of tomorrow: towards a Digital Networks Act"

1. INTRODUCTION

A cutting-edge digital network infrastructure is the foundation for a flourishing digital economy and society. Without advanced digital network infrastructures, applications that make our lives easier will not emerge and consumers will be deprived of the benefits of advanced technologies. Only with the highest performance of such infrastructures, for example, will cars be able to communicate between each other, doctors able to care for patients at a distance rapidly and safely, drones able to improve harvests and reduce water and pesticide use, while connected temperature and humidity sensors enable real-time monitoring of the conditions in which fresh food is stored and transported to the consumer.

There are also many examples across the economy of how enterprises need advanced connectivity and computing infrastructures for the processing of data closer to their operations and to their customers, to use or provide innovative applications and services. This is especially important for applications that require real-time data processing, such as Internet of Things (IoT) devices, autonomous vehicles, and smart grids, and to reduce latency for applications related to predictive maintenance, real-time monitoring, and automation, leading to more efficient and cost-effective operations. Advanced digital network infrastructures and services will become a key enabler for transformative digital technologies and services such as Artificial Intelligence (AI) Virtual Worlds and the Web 4.0, and for addressing societal challenges such as those in the fields of energy, transport or healthcare.

The future competitiveness of all sectors of Europe's economy, therefore, depends on these advanced digital network infrastructures and services, as they form the basis for global GDP growth in the trillion Euro range[1] and the digital and green transition of our society and economy. There is a correlation between the increased deployment of fixed and mobile broadband and economic development[2]. Higher speeds and new generations of mobile networks have a positive impact on GDP[3]. Similarly, as far as submarine cables are concerned, studies show that newly deployed submarine cables can boost GDP[4].

In parallel, digital networks are undergoing a transformation where connectivity infrastructure is converging with cloud and edge computing capabilities. To harness this transformation, the electronic communications sector needs to expand from the traditional consumer internet market towards digital services in key economic sectors, such as the Industrial Internet of Things (IIoT). Moreover, similar to the electronic communications service sector, the equipment sector also faces major technological transformations, in particular due to the trend towards software and cloud-based networks and open architectures. Such convergence of the electronic communications and IT ecosystems brings opportunities for lower cost and innovative services, but also new risks of bottlenecks and dependencies in the field of cloud

---

1 Connected World: An evolution in connectivity beyond the 5G evolution, McKinsey 2020 available at https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/connected-world-an-evolution-in-connectivity-beyond-the-5g-revolution

2 Analyzing the Economic Impacts of Telecommunications (utilitiesone.com) for an overview and How BroabWorld Bank Document, https://etno.eu/downloads/reports/europes internet ecosystem. socio-economic benefits of a fairer balance between tech giants and telecom operators by axon for etno.pdf, ITU, How broab; Impact of broadband speed on economic outputs: An empirical study of OECD countries, Chatchai Kongaut, Erik Bohlin

3 Specifically, mobile's baseline connectivity impact increases by about 15% when connections are upgraded to 3G. For connections upgrading form 2G to 4G, the impact increases by approximately 25%., Mobile technology: two decades driving economic growth (gsmaintelligence.com)

4 https://copenhageneconomics.com/publication/the-economic-impact-of-the-forthcoming-equiano-subsea-cable-in-portugal/

infrastructure and services as well as leading chip platforms[5]. To ensure economic security it is therefore of utmost importance that innovation in this field continues to be driven in the Union and led by its industry. To achieve this, in the current geopolitical context, the Union needs to leverage its current strength in the network equipment supply market with two of the three global suppliers being European.

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[6]. The necessary investments are massive[7]. As further discussed in this White Paper, a modern regulatory framework that incentivises the transition from legacy copper networks to fibre networks, the development of 5G and other wireless networks and cloud-based infrastructures as well as the ability to scale up within single market is key to ensuring that Europe has the advanced communications and computing infrastructure it needs. Short of that, the EU risks missing its 2030 digital targets and falling behind other leading regions as regards competitiveness and economic growth and related user benefits.

Finally, recent geopolitical developments highlighted the importance of security and resilience of infrastructures against both man-made and natural hazards, as well as the complementary role of all types of connectivity including terrestrial, satellite and submarine solutions, for uninterrupted availability of service under all circumstances. In a rapidly changing security landscape, a strategic Union-wide approach to security and resilience of critical digital infrastructures is essential, building on the solid existing legislative framework[8].

Against this background, this White Paper identifies challenges and discusses possible scenarios for public policy actions that aim to build the digital networks of the future, master the transition to new technologies and business models, meet future connectivity needs of all end users, underpin competitiveness of our economy and ensure secure and resilient infrastructures and the Union's economic security.

2. TRENDS AND CHALLENGES IN THE DIGITAL INFRASTRUCTURE SECTOR

2.1. Europe's connectivity infrastructure challenges

The connectivity infrastructure of the Union is not yet ready to address the current and future challenges of the data-driven society and economy and the future needs of all end users.

On the supply side, the 2023 Report on the state of the Digital Decade[9] underlines in particular limited fibre coverage (56% of all households, 41% of households in rural areas)[10] and delays

5 Cybersecurity of Open Radio Access Networks, Report by NIS Cooperation Group, May 2022.

6 This was also acknowledged in the Digital Decade Policy Programme 2030 (Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, OJ L 323, 19.12.2022, p. 4.). According to its Art. 4(2)(a), by 2030 all end users at a fixed location should be covered by a gigabit network up to the network termination point, and all populated areas should be covered by next-generation wireless high-speed networks with performance at least equivalent to that of 5G, in accordance with the principle of technological neutrality.

7 https://digital-strategy.ec.europa.eu/en/library/investment-and-funding-needs-digital-decade-connectivity-targets.

8 See the revised Directive on measures for a high common level of cybersecurity across the Union (NIS2) and the Directive on the resilience of critical entities (CER), both of which entered into force on 16 January 2023, as well as the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure of 8 December 2022.

9 https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade.

10 https://digital-strategy.ec.europa.eu/en/library/broadband-coverage-europe-2022.

in the deployment of 5G standalone networks in the EU. Current trends concerning the trajectories for the digital infrastructure targets laid out in the Digital Decade Policy Programme 2030[11] are a cause for concern. As regards fibre coverage, progress beyond 80% by 2028 does not seem likely, putting the achievement of the 2030 target of 100% in doubt. In comparison to the 56% fibre coverage in the EU in 2022, the US had 48.8%, and Japan and South Korea each reached 99.7%[12].

As regards 5G roll-out, while basic 5G population coverage in the EU currently stands at 81% (with only 51% coverage of the population in rural areas), this metric does not reflect the delivery of actual advanced 5G performance. If we look at prospects for deployment ensuring high reliability and low latency, which are key enablers for industrial use cases, the situation is even worse. The deployment of 5G stand-alone networks can be estimated at significantly less than 20% of populated areas in the EU. Although there is progress on early-stage trials, operators have launched this architecture only in a small number of Member States and limited to some cities[13]. Such limited deployment could, among others, be related to the early stage of 3.6 GHz band deployment. Coverage by 5G in this mid-band, that is needed for higher speeds and capacity, currently stands at only 41% of the population, and mostly this is not in combination with stand-alone deployment. Also, while basic 5G coverage is relatively similar in the largest Member States compared to the US, other regions such as South Korea and China are far ahead. According to the 5G Observatory's International Scoreboard, South Korea has deployed more than five times the number of 5G base stations per 100,000 inhabitants than the EU, and China almost the triple[14].

On the demand side, the take-up of at least 1 Gbps broadband is very low (at 14% in 2022 at EU level) and just above half of all EU households (55%) have adopted at least 100 Mbps broadband. The take-up of high-speed fixed broadband subscriptions is lower in the EU than the US, South Korea or Japan[15]. Mobile broadband take-up is better and lies at 87%, despite almost ubiquitous coverage with at least 4G networks.

These delays represent a critical vulnerability for Europe's economy as a whole, as the delivery of advanced data services and AI-based applications depend on them. The same applies to the deployment of edge computing infrastructure, another key enabler for time critical applications and computing capabilities in relation to real-time data-intensive use cases and IoT. There is a strong correlation between the deployment of capable digital networks and the take-up of modern technologies, which are currently not developing at large scale. The Digital Decade Policy Programme sets out a target of 10,000 climate-neutral highly secure edge nodes to be deployed by 2030 as well as targets for adoption of digital technologies, such as cloud, big data and AI, by European companies. The 2023 Report on the state of the Digital Decade underlined the risks for the achievement of these targets. Edge computing is still at its infancy in Europe.[16] Under current trends, and without further investment and incentives, the targets will not be met by 2030: only 66% of businesses will use cloud, 34% big data and 20% AI, far from the 75% objective set for 2030.

---

[11] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, OJ L 323, 19.12.2022, p. 4.

[12] See Global Fibre Development Index 2023, Omdia

[13] 5G Observatory Biannual Report October 2023, page 8, https://5gobservatory.eu/wp-content/uploads/2023/12/BR-19_October-2023_Final-clean.pdf

[14] 5G base stations per 100,000 inhabitants: 419 (South Korea), 206 (China), 77 (EU), 118 (Japan), 30 (USA).

[15] Cf. International DESI (to be published)

[16] Report on the state of the Digital Decade 2023, SWD Digital Decade Cardinal Points, section 2.4.

While it is necessary to speed up the take-up of new technologies and services, it will not be possible without networks capable of expanding and maturing. Modern digital networks would stimulate the development of new use cases, creating business opportunities contributing to the digital transformation of Europe. Hence, the impact of missing the Digital Decade digital infrastructure targets would be far-reaching, going beyond the scope of the digital sector, and would lead to missed opportunities in innovation areas such as automated driving, smart manufacturing, and personalised health care.

2.2. Technological challenges

New business models and entirely new markets are emerging from technological developments around the App Economy, IoT, Data Analytics, AI or new forms of content delivery such as high-quality video streaming. These applications require a continuous exponential increase in performance of data processing, storage, and transmission. The ability to process and transport large amounts of data across the entire global Internet has led to the remote storage and processing of data in the cloud, between the cloud and the end-user through Content Delivery Networks (CDNs), and close to the end-user with edge computing. Applying this trend to electronic communications networks has led to the virtualisation of network functions in software and the ability to move these functions to the cloud or the edge.[17]

These transformative technological developments create a model of network and service provision that relies not only on traditional electronic communications equipment, network and service providers but also on a complex ecosystem of additional players, including cloud, content, software and component suppliers, amongst others. The traditional boundaries between these various actors are increasingly blurred as they form part of what can be described as a computing continuum ranging from chips and other components for high-speed processors up to AI-powered applications managing the network up to its edge.

One example is the car of the future, which will be far removed from its traditional predecessor, using advanced microelectronics, sensors and software to function, and relying on high-speed and low-latency communication such as 5G to ensure that it communicates with other vehicles and with infrastructure in real time. The ability to quickly and securely transmit data about road conditions, traffic, and potential hazards contributes to overall road safety, while the local processing of data using edge computing allows vehicles to contribute to traffic management by making real-time decisions based on their immediate surroundings. This can help in optimizing traffic flow and reducing congestion.

Another example is the use of cost-efficient 6G connectivity in order to reach a very high share of the population and provide advanced e-health services. In order to offer advanced health monitoring and e-health care in remote areas on the basis of only using low-cost devices, it will be necessary to migrate functionality and artificial intelligence to the network which should be

[17] This technological shift and new paradigm have been confirmed by the large majority of respondents to the Commission's exploratory consultation launched last year to gather views and identify Europe's needs in terms of connectivity infrastructure to lead the digital transformation. In particular, respondents identified network virtualisation, network slicing, and Network as a Service, as the technological breakthroughs that will have the largest impact in the coming years. These technologies are expected to drive the shift from traditional electronic communications networks to cloud-based, virtualised, software-defined networks, reducing costs, improving the resilience and security of networks, and introducing new, innovative services, while transforming ecosystem and business models.
The results of the exploratory consultation were published in October 2023 and are available at: https://digital-strategy.ec.europa.eu/en/news/consultation-electronic-communications-highlights-need-reliable-and-resilient-connectivity.

located as close to the user as possible.[18] Other technologies that could be part of the health care system of 2030 are sensor-based monitoring, extended reality (XR) and drones.

This technological change triggers the emergence of new business models in the electronic communications services sector. The increasingly complex network operations push companies in different segments of the value chain to work together at the infrastructure layer while competition at the service layer becomes more complex. Main trends include network sharing, the separation of infrastructure and service and the creation of service platforms based on concepts like Network as a Service (NaaS) and IoT. NaaS creates a common and open framework between operators to make it easier for developers to build apps and services in partnership with large cloud providers and content application providers (CAPs) that seamlessly communicate with each other and work for all devices and customers. Combined with network slicing solutions, electronic communications operators could be in a position to enable new innovative applications based on quality-of-service levels.

These changes are being gradually introduced to exploit the full potential of 5G networks, especially for industrial sectors outside of electronic communications, the so-called 'verticals' such as manufacturing or mobility. With its successful industry and public-private partnerships, the EU is currently leading (together with China) the development of these future industrial applications of 5G in vertical industry sectors. Examples include a set of operational campus networks, e.g. in factories, ports and mines[19] as well as the ongoing deployment of 5G corridors along EU transport paths[20]. Such changes will be key building blocks of the future 6G computing continuum, which is currently still at the development stage, but which will create further realignment of networks and business cases, and further investment requirements for operators.

The established cloud capacities could also be leveraged to offer more general cloud services for electronic communications, also known as "Telco Cloud", as envisaged in the Industrial Technology Roadmap of the European Alliance for Industrial Data, Edge and Cloud.[21] An EU Telco Cloud could become a major enabler for the rapidly growing markets for IoT-related products and services in the EU and the transition to an industrial Internet enabling critical services in a broad range of sectors and activities of great benefit to citizens, from healthcare to mobility and smart energy grids and as key enabler for the twin transition.

Nowhere is that more obvious than in the city and large urban environments where these sectors and activities come together. The data that they generate can be processed and combined where it is needed, to provide more efficient management of resources, the real-time orchestration of mobility and services, and the optimisation of health and medical care for the citizen. If the different actors in this ecosystem work together, the Telco Cloud would potentially develop a new generation of Operating Systems capable of managing networked resources, such as smart

[18] Hexa-X project, deliverable Deliverable D1.2 Expanded 6G vision, use cases and societal values – including aspects of sustainability, security and spectrum, https://hexa-x.eu/wp-content/uploads/2022/04/Hexa-X_D1.2_Edited.pdf

[19] 5G Observatory biannual report October 2023, Omdia's Mobile Infrastructure Intelligence Service

[20] https://digital-strategy.ec.europa.eu/en/policies/cross-border-corridors

[21] European industrial technology roadmap for the next generation cloud-edge offering, May 2021 [https://ec.europa.eu/newsroom/repository/document/2021-18/European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf]

cities, as well as providing a common interface to develop data- and compute-intensive AI applications.

However, this inevitable opening of the traditionally "closed" electronic communications network in a NaaS approach exposes network capabilities to third parties and bears the possible risk of large non-EU providers becoming leading players in such ecosystems. In the current geopolitical context and from an economic security point of view, this would constitute a significant risk of dependence on non-EU players in the whole digital service sector. It is therefore key that European players develop the necessary capacities and scale to master the transition to service platform providers and face global competitors on a level playing field.

There are vast opportunities in particular for EU equipment suppliers. The ability of European suppliers to seize them and become leading global providers of 6G equipment will largely depend on how they navigate the broad technological changes in the industry and embrace the paradigm shift that comes with them (see section 2.4.1).

To conclude, the sectors of European electronic communications networks and services and network equipment stand currently at cross-roads, either they will embrace and endorse technological transformation, or they will lag behind and leave space to new players largely from outside the EU, with consequences in terms of EU economic security.

2.3. Challenges of achieving scale in EU connectivity services

2.3.1. Investment needs

According to a recent study conducted for the European Commission,[22] reaching current Digital Decade targets for Gigabit connectivity and 5G may require a total investment of up to EUR 148 billion, if fixed and mobile networks are deployed independently and a "full 5G" - offering European citizens and businesses the full capabilities that can be offered by 5G mobile networks - is deployed. A further EUR 26-79 billion of investments may be required under different scenarios to ensure full coverage of transport paths including roads, railways, and waterways, bringing the required total investment needs for connectivity alone to over EUR 200 billion. While in 5G, despite the densification needs to ensure highest performance, EU operators are focussing on reusing existing sites for low and mid-band deployments, in future upgrades, e.g. for 6G or WiFi 6 by the end of the decade, the required network densification is likely to increase, at least in hot spots, by a factor of 2-3 as compared to previous generations. This will therefore further increase the investment needs. Beyond terrestrial connectivity, further investments are required for the integration of advanced satellite services providing complementary solutions for backhaul or even device connectivity in certain remote areas not covered by other more performant and affordable technologies.

Beyond traditional network infrastructure investments to provide for network elements for data transmission, network operators are currently introducing software and cloud-based solutions to provide NaaS. The successful completion of this transformation would require additional significant investment capacities. There is an estimated cloud investment gap in the EU of EUR 80 billion until 2027.[23] In comparison, the annual investments of the largest cloud platform

[22] https://digital-strategy.ec.europa.eu/en/library/investment-and-funding-needs-digital-decade-connectivity-targets.

[23] European Alliance for Industrial Data, Edge and Cloud: "European industrial technology roadmap for the next-generation cloud-edge".

providers in cloud capacities are estimated in the order of EUR 150 billion.[24] A slow transition of EU players towards cloud-based solutions for electronic communications services and beyond would present risks of further dependencies in the area of digital services.

2.3.2. Financial situation of the EU electronic communications sector

In a context of the significant investments needs, the current financial situation of the EU electronic communications sector requires a careful assessment and raises the question whether the telcos will be able to find the funding for the substantial investments that are needed to catch up with the technological shift and future needs.

The EU electronic communications sector is characterised by lower average revenue per user (ARPU) compared to other geographical areas[25] and declining Return on Capital Employed (ROCE),[26] and during the last decade stocks of European electronic communications networks and services providers have underperformed in both global electronic communications indices and European stock markets.[27] European providers of electronic communications networks and services also face low enterprise value/EBITDA multiples, representing a lack of market confidence in the potential for sustainable long-term growth in revenues.

Against this background, the proportion of electronic communications operators' net debt over their EBITDA has continued to grow. In addition, access to finance has degraded as interest rates jumped from historical lows and widespread risk aversion linked to the new global crises result in macroeconomic uncertainty. This has also led investors to focus on fewer and safer projects. The riskier investments are postponed. The increased interest rates have had a significant impact on providers of electronic communications networks. As other infrastructure providers, those of electronic communications networks will need to recover the costs over several decades and even a slight change in the interest rate will impact the financial viability of the investment project. However, compared to other infrastructure investments which are not exposed to overbuilding , certain network operators and private investors argue that investments in electronic communications infrastructure are becoming less attractive.

In this context, perception of attractiveness of advanced digital networks by private investors is of crucial importance for the future of connectivity. Investors have underlined that, at a time of higher inflation, mobilising private investments requires a clear business case for profitability and higher margins compared to what is currently offered. Profitability depends on the take-up of networks, and take-up of enhanced fixed and mobile networks is linked to the development and increased take-up of data intensive applications and use cases, e.g. based on edge

---

[24] Synergy Research Group, e.g. based on Q1/2023 data, Investments related to general cloud capacities tailored to the business model of each cloud provider and not significantly overlapping with the general EU connectivity investment needs.

[25] Average Revenue Per User (ARPU) in Europe continues to trail all global peers. In 2022, mobile ARPU was EUR15.0 in Europe, as opposed to EUR42.5 in the USA, EUR26.5 in South Korea, and EUR25.9 in Japan. In 2022, fixed broadband ARPU was EUR22.8 in Europe, as opposed to EUR58.6 in the USA, EUR24.4 in Japan, and EUR13.1 in South Korea. ETNO, 2024 State of the Digital Communication Report. Global comparisons of ARPU for mobile services can be found in series of ITU Measuring the Information Society Reports, last published in 2018 (https://www.itu.int/pub/D-IND-ICTOI). There, the EU is significantly below the US and Canada and also below other developed countries, yet also ahead of the rest of the developing world.

[26] As regards fixed markets, according to the 2023 State of the Digital Communications ETNO report, the ARPU of ETNO members was at EUR 21.8 compared to EUR 50.6 in the US and EUR 26.2 in Japan, and only ahead of South Korea (EUR 13) and China (EUR 4.9).

[27] State of Digital Communications 2023, ETNO.

computing, AI, and IoT, which, as mentioned above, are still below 2030 Digital Decade target trajectory.

In addition, recent declines in credit ratings signal increased financial risk for the companies concerned. Under the prudential regulation, higher risk translates into increased capital requirements for the financial institutions investing in providers of electronic communications networks. This makes it more costly for banks to grant loans to riskier electronic communications companies.

Some investors also referred to challenges in complying with the prudential rules for banks and insurance companies that inhibit the deployment of capital and the stimulation of equity markets. They argue for reducing the levels of required capital set by the legislative framework on prudential regulation. For example, the Solvency II directive encourages insurance companies to reduce their exposure to equities for prudential reasons[28] as equity prices are volatile. As a consequence, more equity investment arguably leads to lower solvency ratios[29]. The current review of the Solvency II framework might allow capital relief thanks to a reduction of the risk margin and the definition of clear criteria for long-term equity, investments such as infrastructure ones would therefore fully benefit from lower capital requirements.

Nonetheless, since equity invested in unlisted stock such as innovative businesses and new electronic communications operators are still likely to be deemed riskier, some stakeholders signal that they may apply for public support as a catalyst.

Investors also consider that public support, in particular from the Recovery and Resilience Facility and other EU funds (Next Generation EU, Structural Funds, Connecting Europe Facility (CEF), etc.) will help reach the more remote areas, where demand is insufficient to adequately remunerate private deployment. At the same time, in investors' view, public-private partnerships, where the public capital takes the form of guarantees or junior co-investment, are a good and efficient way to help the private sector fund deployment, especially in economically challenging areas. However, the larger part of the investment needs outside remote areas referred to above might need to be assessed on a case by case basis to determine whether it results from a market failure.

Also, in this context, some stakeholders underlined the need for demand-side measures. However, the timing and design of such measures requires careful assessment to ensure their effectiveness in promoting the uptake of broadband services and to avoid that the funds made available remain underused.

Finally, beyond the decreasing profitability levels, investors explained that another element hindering the attractiveness of the European electronic communications market for large investors and big funds is its fragmentation and hence the lack of assets with sufficient scale. The largest investors have minimum threshold for their investments because of their limited capacity to manage and/or monitor their portfolio. This means there are less financiers competing for smaller investments than for larger ones, resulting in less favourable conditions. Further, the relative cost of administering large investments is lower than for smaller ones thus investors can offer better conditions (i.e. lower expected return). Increasing the size of investments projects can reduce the financing costs and make projects feasible that would

[28] Financer la quatrième révolution industrielle, Philippe Tibi, 2019

[29] Deloitte Belgium and CEPS for the European Commission, DG for Financial Stability, Financial Services and Capital Markets Union, Study on the drivers of investments in equity by insurers and pension funds, December 2019

otherwise not be financially viable. One reason for the smaller size of European investment opportunities, compared to the US, is the fragmented nature of the European telco markets. The integration of national markets could be an opportunity to tap into a larger potential pool of investors and financing conditions for electronic communications investments.

2.3.3. Lack of single market

At present, the EU does not have a single market for electronic communications networks and services, but 27 national markets with different supply and demand conditions, network architectures, different levels of very high-capacity networks coverage, different national spectrum authorisation procedures, conditions and timing, as well as different (albeit partly harmonised) regulatory approaches. The fragmentation does not only concern the supply side of the market. Also from the demand, i.e. end-users' side, market conditions differ from one Member State to another. The fragmentation of the single market for electronic communications was underlined by the majority of respondents to the explanatory consultation who also highlighted that the removal of obstacles, notably burdensome sectoral regulation, can create incentives for cross-border consolidation and emergence of a fully integrated Digital Single Market. Concerning the barriers to market integration, the majority of the respondents to the exploratory consultation called in particular for a more integrated spectrum market and a more harmonised approach to spectrum management across the EU. They suggested that it would be appropriate to align the approaches related to, for example, duration of licences, reserve prices, annual costs of spectrum, or spectrum sharing practices.

Radio spectrum policy is an area of shared competence between the EU and Member States. The EU has adopted rules, in particular for the harmonisation of technical conditions for the use of spectrum. Member States' action has focused on the implementation of spectrum authorisation, management and use. However, the way spectrum is managed and used in one Member State has an impact on the internal market as a whole, for example through disparate starts in the development of new wireless technologies or new services or by creating cross-border interferences, with further possible repercussions for EU competitiveness, resilience and technological leadership. Therefore, it is imperative that spectrum is managed in a more coordinated way among all Member States to maximise its social and economic value.

The past attempts towards more EU coordination, convergence and certainty in spectrum management, for example, in the context of the proposal for a Telecommunications Single Market regulation and the European Electronic Communications Code (hereinafter referred to as the "Code")[30], were not successful in many respects. Ultimately this has resulted in detrimental consequences for the EU as a whole. For example, the authorisation process for bands anticipated to enable future 5G deployment started in 2015 in the first Member States and is not yet fully completed now in 2024, despite the deadlines set by the Code. The authorisation of the use of the 2.6 GHz band for 4G took 6 years for 26 Member States and even 10 years for 27 (despite the absence of an exceptional pandemic event as for 5G). This has resulted in fragmented 4G and 5G roll-out landscapes across the EU, where some Member States were almost one wireless technology generation behind others[31].

[30] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018, p. 36.

[31] Commission study on assessing the efficiency of radio spectrum award processes in the Member States, including the effects of applying the European Electronic Communications Code (https://digital-strategy.ec.europa.eu/en/library/study-assessing-efficiency-radio-spectrum-award-processes-member-states-including-effects-applying).

Moreover, where spectrum bidders ended up overpaying, this has been associated with a reduction in investment capacities and delays in services deployment by providers of electronic communications networks and services. Ultimately, it is the consumers and business users who have paid the price in terms of suboptimal quality of services, which ultimately negatively impacts EU's economic growth, competitiveness and cohesion.

There are also national rules beyond sector specific electronic communications legislation imposing obligations, as regards, for instance, network security, lawful interception, data retention or localisation of Security Operations Centres, that were also raised in the explanatory consultation as barriers to the full integration of the Single Market. In these areas, EU law allows for a significant margin for national legislators to impose obligations, which has resulted in significant fragmentation (e.g. different duration of data retention obligations, localisation requirements for network operation centres, lack of mutual recognition for security vetting for relevant staff) preventing a provider operating a network in more than one Member State from exploiting economies of scale.

The fragmentation of the EU market for electronic communications networks and services along national borders could impact the ability of operators to reach the scale needed to invest in the networks of the future, in particular in view of cross-border services, important for an effective deployment of IoT, and a more centralized operation.

While there are around 50 mobile operators, and more than 100 fixed operators in the EU, only few European operators (e.g. Deutsche Telekom, Vodafone, Orange, Iliad and Telefonica) are present in several national markets. When it comes to mobile markets, at service level, 16 Member States have three mobile network operators, nine Member States have four and two Member States have five. In certain Member States, in terms of distinct mobile electronic communications network infrastructures, the number is lower than the number of service providers due to existing network sharing arrangements (e.g. in Denmark or Italy). Even the mobile operators that are part of corporate groups with a large footprint across the EU operate within national markets and do not seem to harmonise their offerings and operational systems at EU level, due to the inherently different market and regulatory landscapes, beyond the need to ensure affordability in Member States with lower purchasing power.

Against this backdrop of fragmentation in the EU (which is considerably higher than in other regions of the world, such as the US) and lower profitability levels, the question arises as to whether cross-border consolidation or different forms of cooperation upstream could allow operators to acquire sufficient scale, without compromising downstream competition. Some operators are of the view that there are no obstacles to cross-border consolidation other than the net negative efficiencies and synergies (despite expected cost reductions which could be allowed by more centralised operations, especially in virtualised networks) due to fragmented regulatory conditions.

While prices differ considerably between Member States,[32] mobile and fixed broadband prices are typically lower in the EU compared to the US for the vast majority of tariffs, bringing significant short-term consumer benefits. Still significant differences in prices remain between Member States, due to the inherently different market and regulatory landscapes, beyond the need to ensure affordability in Member States with lower purchasing power. While the single

[32] Mobile and fixed broadband prices vary widely across the EU not only in nominal terms but also at power purchasing parity. See European Commission, Directorate-General for Communications Networks, Content and Technology, Mobile and fixed broadband prices in Europe 2021 – Final report and executive summary, Publications Office of the European Union, 2022, available at https://data.europa.eu/doi/10.2759/762630.

market thus, on average, delivered on price, it did not deliver on the deployment of advanced infrastructures and services like 5G standalone, as it remains slow[33], which means that business users today in the EU do not have access to advanced industrial and IoT services as well as commercial private networks. In the future, the issue of quality of services offered also for consumers will became much more important due to new use cases. Besides potential immediate solutions to restrict unjustified discrimination, cross-border services and networks in the EU could be a sustainable solution with much broader benefits in terms of reach and quality both for consumers and business users.

2.3.4. Convergence and level playing field

The convergence of electronic communications networks and services and cloud infrastructures does not only concern the infrastructure layer, but also the service operations. As explained in section 2.2 above, connectivity markets are facing transformative technological developments the result of which will be both a converged supply (i.e. network and service provision) as well as a converged demand by end-users. 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 said converged ecosystem should not fall under equivalent rules applicable to all players and whether the demand side (i.e. end-users and in particular consumers) should not benefit from equivalent rights.

Currently, the existing EU regulatory framework for electronic communications networks and services does not establish obligations related to the activities of cloud providers and does not regulate the relationship between the various players in the new complex digital infrastructure ecosystem. More specifically, the cloud infrastructure and services provision are not in the scope of the Code (contrary to the recent NIS2 Directive[34] for instance). Even though cloud providers run large (backbone) electronic communications networks, these networks are exempted from parts of the electronic communications regulatory framework, regulatory oversight and dispute resolution. More than 60%[35] of the international traffic transits through submarine cables, which do not belong to "public electronic communication network operators" within the meaning of the Code. Moreover, large cloud providers operate their own backbone networks and data centres and hand over the traffic deep into the networks of said public electronic communication network operators. Consequently, traffic transits mostly on private networks, which are largely unregulated, rather than on public ones. Some of the largest Internet players send large amounts of traffic, but hardly receive any IP traffic in return[36].

Another distinction made in the Code is between the kind of service provided: for example, most obligations apply to Internet Access Service and to Number-based Interpersonal Communications Services (NBICS) while Number-independent Interpersonal Communications Service (NIICS) are subject to only a few obligations and are exempt for instance from

[33] 2023 Report on the state of the Digital Decade, https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade

[34] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, p. 80.

[35] BoR (23) 214, Draft BEREC Report on the general authorization and related frameworks for international submarine connectivity.

[36] Depending on what type of hyperscaler it is estimated that the ratio of the difference between IP traffic sent, and IP traffic received is in the magnitude of around 20 or more.

contribution to the funding of the Universal Service or the financing of sector regulation. Whilst both NIICS and cloud computing services are within the scope of the Digital Market Act[37], those rules only apply to gatekeepers designated for these specific core platform services.

2.3.5. Sustainability challenges

The ICT sector accounts for between 7% and 9% of global electricity consumption (forecast to rise to 13% by 2030),[38] around 3% of global greenhouse gas emissions,[39] and increasing amounts of e-waste. Yet, if properly used and governed, digital technology can help cut global emissions by 15%[40], outweighing the emissions caused by the sector. For instance, smart building design has the potential to generate energy savings of up to 27%[41] and smart mobility applications have been shown to be able to reduce transport emissions by up to 37%.[42] Connected and Automated Mobility is expected to be one of the main drivers to decarbonise the transport sector and 5G is expected to be one of its main enablers. However, significant further efforts are needed to apply digital technology systematically and make sure it powers solutions carefully designed according to circular, regenerative principles.

The "softwarisation" and "cloudification" of the next generations of electronic communications networks hold the promise of efficiency gains for all sectors, but also present new challenges in terms of energy consumption (e.g., Open RAN (radio access network) in cellular networks). Increased energy consumption due to step changes in traffic load has a cost in itself that has significantly increased in recent years with rising energy prices. At the same time, high energy costs could incentivise investments into more energy-efficient and low-carbon network operations and technologies with less e-waste.

Modern digital networks can contribute significantly to advancement of sustainability. Concrete examples include the deployment and adoption of new and more efficient technologies such as fibre, 5G and 6G, the phasing out of legacy fixed and mobile networks. Also, the use of more efficient codecs (coders-decoders)[43] for data transmission is essential. Newer generation video codecs are inherently more sustainable by minimizing outgoing energy and power at the same video quality.

2.4. Need for security in the supply and in the operation of networks

2.4.1. Challenge of trusted suppliers

In a geopolitical environment increasingly marked by tension and conflict, the growing requirement for security and resilience of key enabling communications technologies and critical infrastructures highlights the need to rely on trusted suppliers, in order to prevent vulnerabilities and dependencies, with potential knock-on effects that put the entire industrial

[37] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, p. 1.

[38] Strategic Foresight Report 2022; EU Action Plan on Digitalising the Energy System.

[39] The Shift Project, "Déployer la sobriété numérique", October 2020, p. 16; World Bank 2022

[40] World Economic Forum 2019.

[41] https://www.buildup.eu/en/news/overview-smart-hvac-systems-buildings-and-energy-savings-0

[42] TransformingTransport.eu, EU-funded Horizon 2020 Big Data Value Lighthouse project.

[43] A codec is a process that compresses large amounts of data – most commonly a video stream - before their transmission and decompresses them after the reception.

ecosystem in jeopardy. The EU 5G Cybersecurity Toolbox[44] for example put forward a set of recommended measures to mitigate the risks to 5G networks, notably the assessment of the risk profile of suppliers and the application of restrictions for suppliers considered as high risk, including necessary exclusions from key assets. In this respect, in its Communication of 15 June 2023 on the "Implementation of the 5G Cybersecurity Toolbox"[45] the Commission confirmed that decisions adopted by Member States to restrict or exclude Huawei and ZTE are justified and compliant with the 5G Toolbox.

This creates a need to fill any gaps left by these high-risk vendors in the supply chain with new capacities provided by existing or new actors. In this context, Research & Innovation (R&I) efforts in key technologies relevant for secure communications networks will have to be stepped up to ensure that a sufficient level of intellectual property and production capacity remains available across the entire EU supply chain, at all times. The objective is not only to ensure that the EU remains among the global leaders in communications systems but also to achieve leadership in the development of new capabilities in related areas such as edge clouds and swarm computing, radio frequency identity chips technology, quantum communications, quantum resilient cryptography, and submarine cable infrastructures.

2.4.2. Security standards for end-to-end connectivity

To achieve the highest security and resilience the EU should also lead the development of security standards covering the entire value stack, from end-to-end and from the hardware layer up to the service layer (e.g. secure messaging and videoconferencing standards). The challenge for the EU is to ensure that such developments across the EU result in common and interoperable security standards for all key infrastructural elements underpinning the sensitive communications infrastructures of all Member States. The Commission's initiative to establish an EU Critical Communication System (EUCCS) to connect all security and safety responders in Europe in order to allow for seamless critical communication across the Schengen area will be a key building block in this regard.

The new digital era will be based, among others, on quantum technologies for secure connectivity and quantum computing. Communication networks and the way data are protected will experience a paradigm shift as a direct consequence of advances in quantum computing. As safeguarding our data and securing communication are vital for our society, economy, infrastructure, services, and prosperity, as well as our political stability, we need to anticipate potential threats coming from potential malicious use of future Quantum Computers, which could put our traditional methods of encryption at risk.

The Cyber Resilience Act (CRA), which is set to enter into force later this year, will contribute significantly to securing the EU's digital infrastructure. It places security-by-design obligations on the manufacturers of hardware and software products, covering the whole life cycle of such products from their design and development to their maintenance. The CRA not only covers many of the products deployed in digital infrastructures, such as routers, switches or network management systems, but it also requires the manufacturers of connectable hardware and software products at large to protect the confidentiality and integrity of data by state-of-the-art means. This could entail, where appropriate, the use of quantum-resistant cryptography. To support manufacturers in their implementation, the Commission will request the development

[44] https://digital-strategy.ec.europa.eu/en/news/connectivity-toolbox-member-states-agree-best-practices-boost-timely-deployment-5g-and-fibre

[45] C(2023) 4049.

of European standards by the European Standardisation Organisations. In addition, the recently adopted European Cybersecurity Scheme on Common Criteria (EUCC) will allow manufacturers of technological components, such as chips, to provide security assurance in a harmonised manner under the EU's Cybersecurity Act.

2.4.3. Secure and resilient submarine cable infrastructures

A precondition for secure communications is a higher level of resilience and integration of all communication channels: terrestrial, satellite and, importantly, submarine. In the current context of increased cybersecurity and sabotage threats, governments in all regions are paying particular attention to their potential reliance on critical submarine cables. Indeed, over 99% of intercontinental data traffic is carried through submarine cables, and several islands in Europe are highly dependent on such submarine cables for intra-EU communications.

In this context, in the EU, the Nevers Call of March 2022[46] recognised the utmost importance of critical infrastructure such as electronic communications networks and digital services to many critical functions, and the fact that the latter are a prime target for cyberattacks. The Council in its Conclusions on the EU's Cyber Posture of 23 May 2022 and on the EU Policy on Cyber Defence of 22 May 2023 requested risk evaluations and scenarios to be undertaken. In October 2022, President von der Leyen presented a 5-point plan to enhance preparedness, stress test infrastructure, increase the capacity to respond through the Union Civil Protection Mechanism, make better use of satellite surveillance capacity, as well as strengthen cooperation with NATO and key partners. In its Critical Infrastructure Resilience Recommendation of 8 December 2022, the Council set out targeted, voluntary actions at EU and national level for enhanced preparedness, enhanced response and international cooperation. These actions focus on critical infrastructure with significant cross-border relevance and in identified key sectors, such as energy, transport, space, and digital infrastructure.

In the State of the Digital Decade report 2023, the Commission underlined the importance of making progress towards more resilient and more sovereign networks and in particular to limit the vulnerability of the EU's key infrastructure, including submarine networks. It also issued a clear recommendation to Member States to *"[…] boost their efforts, including through necessary investments, to ensure that European digital infrastructures are secure and resilient, especially backbone infrastructure and submarine cables*". In parallel, Member States have also committed to reinforce Internet connectivity between Europe and its partners, in the Ministerial Declaration on "*European Data Gateways as a key element of the EU's Digital Decade*".

Finally, at the informal TTE Council in León on 23-24 October 2023 and the TTE Council of 5 December 2023, Member States clearly stated that they consider physical damage to underground cables, submarine cables and cable landing points to be the biggest threat to the electronic communications sector. Such damage is usually accidental, but there have been cases of sabotage and interference, and these can be expected to grow given the geopolitical situation. Member States also expressed concern about the capabilities of threat actors and third countries to attack or interfere with suppliers and Managed Service Providers. These actors could seek to exploit vulnerabilities in order to gain access to network management systems, either to intercept communications or to disrupt service provision. In particular, Russia's war of aggression against Ukraine has had a significant impact on awareness about the security of

[46] https://presse.economie.gouv.fr/08-03-2022-declaration-conjointe-des-ministres-de-lunion-europeenne-charges-du-numerique-et-des-communications-electroniques-adressee-au-secteur-numerique/

communications networks, including submarine cables. These concerns are exacerbated by recent cable incidents in the Baltic Sea[47].

In addition, this geopolitical context may warrant a significant increase of investment for secure and resilient connectivity within the horizon of this decade. With less than EUR 2 billion budget for the entire Multiannual Financial Framework, CEF Digital is not sufficient to incentivise private investment to cover these funding needs and may need to be combined where appropriate with other resources, such as other EU programmes and Member State support aimed to address market failures.

3. MASTERING THE TRANSITION TO THE DIGITAL NETWORKS OF THE FUTURE - POLICY ISSUES AND POSSIBLE SOLUTIONS

3.1. Pillar I: Creating a "NextGen Connectivity Hub"

As described in earlier sections, cars communicating with each other, doctors caring for their patients at a distance, and other future applications facilitating business and improving the lives of citizens depend on the availability of high-performing digital infrastructures. These in turn depend on their respective industrial ecosystem, ranging from chips to algorithms, radio equipment to data visualisation. As section 2.2 describes, just as connectivity and computing are converging, so too the companies in these different segments of the value chain need to work together. But the different sectors are fragmented and, as well as lacking scale, they do not have a common approach to the innovation necessary to deliver next generation connectivity and computing.

To ensure that these innovations do happen in the EU and safeguard our economic security requires an ambitious industrial policy. In particular, it is of key importance that EU industry has sufficient technology capacity in key parts of the digital supply chain and is able to reap economic benefits in the most attractive parts of the digital value chain. The goal is to foster a vibrant community of European innovators, creating the "NextGen Connectivity Hub", an ecosystem that spans the whole computing continuum from semiconductors, computational capacity, radio technologies, to infrastructure and applications.

This approach does not mean that everything must be designed and produced in the EU, but that the right balance and synergies have to be found between open trade and the EU's own technological capacity. The "NextGen Connectivity Hub" would be a pillar of a more resilient, balanced and interdependent global system, while ensuring that welfare keeps being created in the EU.

3.1.1. Capacity building through open innovation and technology capabilities

As hybrid networks, edge computing, and full cloud migration change the architecture of connectivity infrastructure, the historical strength of Europe in the network equipment and service industry is at risk. It is therefore important to safeguard EU global leadership in electronic communications network equipment and facilitate the build-up of further industrial capacities in this transition towards cloud-based networks and the integration of telco-edge infrastructures and services. Next to industrial capacity, it is equally important for the EU to strengthen its technological innovation capabilities as well as developing the necessary knowledge and skills. Otherwise, Europe will lag behind, and the equipment and services will

[47] A submarine gas pipeline (between Finland and Estonia) and electronic communications cables (between FI and EE, and between SE and EE) were damaged.

come from elsewhere, with a time delay and a cost premium that will make it harder for SMEs and citizens to avail of the advanced digital services that the data economy has to offer.

EU businesses increasingly partner with non-EU players, both within the electronic communications services ecosystem but also in the supply industry. While such partnerships with actors from like-minded countries can generate synergies and benefits, a potential dependency on a small number of suppliers of critical infrastructures and services, such as cloud, edge, AI tools, or submarine cable infrastructures, bears the risk of new bottlenecks or lock-ins[48]. The goal must be to create an equally strong dynamic for partnership between businesses within Europe.

In the area of semiconductors, the EU has reacted to reverse this trend: with the Chips Act[49], the EU has put forward an ambitious programme which has already mobilised more than EUR 100 billion of public and private investments. But when it comes to connectivity infrastructures, an industrial policy to incentivise investments by EU players and catalyse the ”NextGen Connectivity Hub” to enable future applications is currently missing.

Nevertheless, in the equipment sector, the EU has a solid base that it can build upon. Today, it is the home of two of the three largest suppliers of digital network equipment, both as regards global sales market share and share of standard essential patents. Following decades of success in shaping mobile communication standards and driving innovation in the EU and globally, the challenge is to build on this leading position and leverage it to the broader supply and value chain, such as in the area of cloud computing but also chips, where Europe starts from a weaker position. This extends to complementary infrastructures, such as submarine cables or even non-terrestrial connectivity.

As for production, deployment, and operational capacities, Europe can also build on its strength when it comes to R&I in the upstream part of the digital value chain. The EUs already hosts a solid R&I base for networks, with globally renowned scientific excellence on which future R&I ecosystems can build. The geopolitical context and the trend towards ever more critical applications, such as blockchain in finance, connected trucks in logistics, or telemedicine, call for infrastructure security and resilience by design. These design criteria therefore need to be placed at the forefront of our R&I efforts.

However, the transformation of the EU’s connectivity industry requires significant investment capacities, in particular when compared to the massive investments made by large cloud providers into cloud and AI capacities. There are a number of EU funding instruments and programmes that already support private investments in R&I in relation to the communications sector. These include the Smart Networks and Services Joint Undertaking (SNS JU) under Horizon Europe, but also InvestEU, the Digital Europe Programme (DEP), and the Connecting Europe Facility (CEF) Digital.

The SNS JU is the current EU platform for R&I funding towards 6G systems in cooperation between industry and public actors. One of its main objectives is to leverage the EU’s strength

[49] Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe’s semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act) (Text with EEA relevance)

[49] Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe’s semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act) (Text with EEA relevance)

[50] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6246

in network supply towards the broader value chain including cloud and software as well as devices and components. The SNS JU already addresses several industry-led R&I needs (mostly in anticipation of 6G): research on concepts, architectures and core components of 6G systems, large-scale trials and pilots, standardisation, virtualisation of networks, cloud software, as well as AI-enabled radio access networks. This current scope is, however, too narrow to address the challenges identified and to catalyse the next generation connectivity ecosystem covering the entire computing continuum. Moreover, the existing budget of EUR 900 million for 2021-2027 is limited to R&I and represents a small amount in the face of those challenges.

In December 2023 the Commission approved up to EUR 1.2 billion of state aid by seven Member States for an Important Project of Common European Interest (IPCEI) in Next Generation Cloud Infrastructure and Services (IPCEI CIS), which is expected to unlock additional EUR 1.4 billion in private investments.[50] Already in June 2023, the Commission approved another IPCEI to support research, innovation and the first industrial deployment of microelectronics and communication technologies across the value chain (IPCEI ME/CT), involving 14 Member States, counting with EUR 8.1 billion in public funding, unlocking EUR 13.7 billion in private investments. Leading chip suppliers and network equipment vendors participate, and developing advanced chips for electronic communications networks is an important component of the IPCEI's objectives. However, at this stage, coordination among these and other ongoing initiatives is lacking, hampering synergies and best employment of scarce financial resources.

3.1.2. Way forward

To ensure a more efficient use of resources, the EU needs to establish a coordinated approach to the development of integrated connectivity and computing infrastructures. To do so it is not only necessary to develop a synergetic ecosystem between actors in the different sectors, the "NextGen Connectivity Hub", but also to rethink the interplay and synergies that can be established between existing EU funding programmes. This is necessary in order to maximise the impact of R&I in communications and computing networks, but also capacity building and pre-deployment, especially given the convergence of technologies and services (cloud-edge continuum, AI, connectivity). These programmes should be built around the overall objectives of improving the EU's industrial capacities, of contributing to a secure and resilient connectivity infrastructure, and of bolstering Europe's competitiveness. Ultimately, this should provide the environment for future networks and applications being developed, tested, and deployed in the EU.

The first step towards the "NextGen Connectivity Hub" can be taken by launching a number of large-scale pilots that set up end-to-end integrated infrastructures and platforms and bring together players from different segments of the connectivity value chain. These would be funded under the Horizon Europe programme over the next three years.

Secondly, these pilot infrastructures should be used to test innovative technologies and applications (including demos, proof of concepts and early deployment of technologies). They could be attached where appropriate to the European network of competence centres in semiconductors, which are maximising synergies with the European Digital Innovation Hubs. This would promote exchanges between players from the traditional electronic communications value chain and players along the broader computing continuum, bringing together not just the

[50] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6246

key technologies from startups to large businesses but also researchers and attracting talent to develop knowledge and skills.

Thirdly, Europe can again build on existing initiatives to scale-up innovative technologies and applications. For example, these pilot architectures could be used to trial AI systems and applications funded under the EU's AI flagship, in order to maximise synergies and ensure the capacity of advanced edge connectivity networks to support and in turn be managed by AI applications. Another example is the development of 5G corridors, funded under the CEF Digital programme, where the corridors can be used for testing and piloting new technologies and applications, in particular connected and autonomous driving but also advanced logistics and IoT applications.

Fourthly, the IPCEIs, in particular in the area of microelectronics and connectivity as well as next generation cloud infrastructure and services, can be used to structure innovation and accelerate market take-up. In January 2024, the EU combined its strength in supercomputing with AI in its Communication on boosting startups and innovation in trustworthy AI.[51] Other key ongoing initiatives include Smart Communities under the Connecting Europe Facility Digital (CEF2), telco-cloud convergence under the DEP, and other partnerships, such as Chips for 6G in the Chips JU and 5G Cybersecurity in the European Cyber Security Competence Centre (ECCC). The coordination of these and the related R&I initiatives under Horizon Europe could lead to a number of large-scale priority pilots, around which a vibrant community of European innovators would be created.

To succeed, Europe must mobilise all the relevant actors in a collaborative ecosystem. As well as the 6G Industry Association, the key private sector partners in the SNS JU, the European Alliance for Industrial Data, Edge and Cloud (the Cloud Alliance) brings together actors in the cloud and edge environment. These entities, together with representatives of software and AI applications providers, could take the lead in designing and operating a vibrant and innovative industrial programme.

Concretely in the next few years, the SNS JU could coordinate the creation of immediate synergies with relevant programmes and IPCEIs. Following the publication of this White Paper, the Commission will shortly start developing with stakeholders the specifications of this task, building notably on the ongoing work to develop a European Telco Edge Cloud, as envisaged by the Industrial Technology Roadmap developed by the Cloud Alliance.

In October 2023, the Commission launched a Joint European Forum for Important Projects of Common European Interest (JEF-IPCEI) to focus on identifying and prioritising strategic technologies for the EU economy that could be relevant candidates for future IPCEIs. As part of the JEF-IPCEI, and drawing from the experience under the Chips Joint Undertaking (Chips JU), CEF2, DEP, and relevant national and regional funds, the possibility of supplementing these measures with a new IPCEI to additional target areas along the computing continuum such as chips and artificial intelligence could be discussed.

In the longer term and in order to further leverage EU technology capacities, related areas that are crucial for future networks need to be brought under a single cooperative governance and equipped with the appropriate budget, following the examples of the AI innovation package and the Chips Act, which extended the mandates of respective Joint Undertakings on European High Performance Computing and Chips (EuroHPC JU and Chips JU). The associated future

[51] COM/2024/28 final

research priorities should include security solutions in critical hardware and software modules, interoperability between cloud infrastructures supported by open-source activities, diversified supply chains for products, components, and materials, while strengthening know-how in the EU, and sustainability solutions covering various aspects of the networking domain ("Sustainable 6G") and a variety of the vertical industries, such as manufacturing, transport, energy, and agriculture (i.e. "6G for sustainability").

Increased and better aligned R&I activities that are embedded into an industrial policy and equipped with the appropriate budget will strengthen Europe's technology capacity, create synergies, ensure coherence, and leverage the multiplier effect of EU actions for private investments. It will also provide the means of ensuring the EU's security and resilience in this domain as well as improve cooperation among European players in an ecosystem that spans the whole computing continuum, supporting them to compete on an equal footing with global competitors. The goal should be to establish a single entry point for EU support across the whole continuum from radio frequency to chips to software to algorithms to compute capacity in the transition towards state-of-the-art connectivity 'made in Europe'.

3.1.3. Summary of possible scenarios

- *Scenario 1: The Commission will propose in the forthcoming Horizon Europe Work Programme large-scale pilots that set up end-to-end integrated infrastructures and platforms for telco cloud and edge. In a second step these pilot infrastructures would be used to test innovative technologies and AI applications for various use cases*

- *Scenario 2: The possibility of extending the IPCEI CIS or supplementing it with a new IPCEI could be discussed by the Commission's Joint European Forum for Important Projects of Common European Interest (JEF-IPCEI), which is tasked with identifying and prioritising strategic technologies for the EU economy that could be relevant candidates for future IPCEIs.*

- *Scenario 3: The Commission may consider ways to improve synergies between the Chips Joint Undertaking, Important Projects of Common European Interest, the Connecting Europe Facility and the Digital Europe Programme, tasking the Smart Networks and Services Joint Undertaking (SNS JU) to adopt a coordinating role to support the creation of a next generation connectivity ecosystem. The SNS JU should liaise with the European Alliance for Industrial Data, Edge and Cloud as appropriate.*

3.2. Pillar II: Completing the Digital Single Market

3.2.1. Objectives

One of the main objectives of the Code is to promote connectivity by putting in place a regulatory framework conducive to more investment in very high-capacity networks. With this objective in mind, a number of legal provisions in the area of access regulation and spectrum management were designed to facilitate investment, and to cut red tape. However, despite a number of clear obligations set in the Code, the results were not satisfactory (e.g. co-investment, wholesale only provisions had not been much used in practice). This is due not only to the delayed transposition by several Member States, but also because of the complexity of the framework and its procedures.

While reinforcing investment objectives, the Code also aims at the promotion of competition (both at infrastructure as well as at services), contribution to the development of internal market and promotion of end-user benefits. The assumption is that competition drives investment based on market demand and is to the benefit of consumers and businesses. While all these principles remain valid, recent technological developments and new global challenges call for a possible broadening of objectives by incorporating wider dimensions such as sustainability, industrial competitiveness, and economic security into the policy framework.

Whatever measures might be taken in the future to address said new challenges, end-users' protection, including consumers, will continue to carry important weight among the objectives. Ultimately, as set out in the "European Declaration on Digital Rights and Principles for the Digital Decade" of 15 December 2022, people are at the centre of the digital transformation in the European Union and all businesses, including SMEs, should benefit from it.

3.2.2. Scope of application

In light of the developments described above (see section 2.3.4), and in particular the quick progressing of convergence between electronic communications networks and cloud, a rethinking of the scope of application of the electronic communications regulatory framework could be considered. Currently, an end-user sends or receives data that "travel" via different networks or network segments (ranging e.g. from undersee cables to local access networks) and that are subject to different applicable rules. It is difficult to explain and to justify to an end-user the rationale for such difference in the applicable rules (for instance as regards network security or lawful interception).

At the same time, the recent technological changes create an opportunity for alignment of the operations of electronic communications and cloud services with the development of pan-European core network operators. For example, the cloudification of 5G networks, which is underway, can provide significant benefits to the electronic communications network providers and allow them to leverage the same economies of scale of cloud providers by, *inter alia*, unifying the core network functionality of several national electronic communications networks in the cloud. However, when it comes to electronic communications networks, this integration of functionalities in centralised cloud data centres that provide cross-border core network functionalities currently faces several legal barriers due to non-harmonised legal frameworks in the Member States.

On the service side, a consistent provision of NaaS-based applications relying on standalone 5G core networks, network slicing, and spectrum resources available across Member States could provide a new business case for cross-border operations.

On the network side, it is to be recalled that - in contrast to voice traffic (which is billed according to the "calling party's network pays" principle) - IP interconnection is done on the basis of transit and peering agreements based on a "bill-and-keep" approach where the Internet Service Provider (ISP) does not receive payments at the wholesale level for terminating traffic. The ISP recovers its costs at the retail level by selling internet connectivity to its end users, who "cause" the internet traffic when retrieving data/content offered by CAPs. For supplementary paid peering and for transit, payment is made on the basis of the capacity provided at the point of interconnection. The main recent changes in the overall global architecture of the internet and of interconnection are caused and driven by the expansion of own backbone and delivery infrastructures by the CAPs. This has shifted the relation of interconnection in form of transit

and peering. "On-net" exchange now predominates[52], with the CDNs' cache servers collocated directly in the ISPs' networks, leading to a very direct and cooperative interaction between CAPs and ISPs as they have to agree technically and commercially on the conditions for transit and peering bilaterally (e.g. on the locations of traffic handover, the level of transit prices, on the question of settlement-free or paid peering or on quality and efficiency aspects).

There are very few known cases of intervention (by a regulatory authority or by court) into the contractual relationships between market actors[53], that generally functions well and so do the markets for transit and peering. There has been nonetheless a vivid debate on this topic[54]. Moreover, it cannot be excluded that the number of cases in the future will increase. Should this be the case, policy measures could be envisaged to ensure swift resolution of disputes. For example, the commercial negotiations and agreements could possibly be further facilitated by providing for a specific timeline and by considering the possibility for requests for dispute resolution mechanisms, in case commercial agreements could not be found within a reasonable period of time. In such case, BEREC could be solicited.

3.2.3. Authorisation

The general authorisation regime established in 2002 and maintained in the Code replaced the previous regime of individual licenses/authorisations, by pre-establishing generally applicable conditions for the provision of electronic communication networks and services (ECNS). Yet, given the local character of the physical networks, and the fact that spectrum is deemed to be a national resource (see section 3.2.5), authorisations are subject to conditions established by the Member States' competent authorities and granted and implemented at national level.

Nonetheless, due to cloudification and softwarisation, network provision is less and less linked to location. Furthermore, coverage of wireless networks, such as satellite networks, can extend beyond national – and even EU – borders. While there are still clear benefits in keeping the implementation of authorisation regimes at national level, in particular for local access and retail services, assigning radio spectrum under conditions which differ between Member States may not always be the most efficient approach, in particular for satellite communications. There could therefore be an economic and technical justification for a more European approach.

One of the elements explaining the fast development of information society services has been the fact that they could be provided to the entire EU simply by complying with the legislation of the Member State of establishment ('so called 'country of origin' principle), without the need to comply with the legislation of each Member State in which services are provided. While network virtualisation may technically allow the provision of cross-border core networks and create a market for core network services, the business case cannot develop if there is insufficient scale, or if different regulatory regimes hinder such business case. To develop the business case, setting out a single set of rules by enabling authorisation based on the country of origin principle for providers of core networks and core network services could balance the approach to all types of providers of digital networks and services, putting them on a more equal level. In the converging ecosystem, where a boundary between the "traditional" providers of

[52] Only a few ISPs do not allow on-net data exchange, continuing instead to exchange traffic across network boundaries and point of interconnection.

[53] For an overview of known cases see WIK-consult: Final study report "Competitive conditions on transit and peering markets", Bad Honnef, 28.02.2022.

[54] For an overview of the various arguments raised in this debate, see e.g. also the responses to the relevant section of the exploratory consultation available at: https://digital-strategy.ec.europa.eu/en/news/consultation-electronic-communications-highlights-need-reliable-and-resilient-connectivity

digital networks and services on the one hand and the providers of e.g. cloud services on the other hand becomes increasingly blurred, the regulatory treatment of those services should be more holistic. It could also lessen the administrative burden by bringing in potential rationalisation of reporting obligations of different actors.

The application of a single set of rules based for instance on 'country of origin' principle for core networks and core network services would enable EU core network operators to leverage the full potential of the internal market to reach critical size, take advantage of scale economies, and reduce capital expenditure and operating costs, thus solidifying their financial position, attract more private investments and ultimately contributing to EU sovereignty. In this scenario the applicable legislation and the competent authority to regulate access to networks and retail services provided to end-users would remain the same and the one closest to the end-users, i.e. those of the Member State of the provision of the access network and of the retail service. This would also ensure that the specificities of local markets are adequately taken into account when defining appropriate access remedies and when guaranteeing the highest level of protection of end users.

3.2.4. Addressing barriers to core network centralisation

In addition to the sector-specific regulatory barriers mentioned above, contributors to the exploratory consultation listed other regulatory barriers to the establishment of a true Digital Single Market such as different obligations across the EU with regard to network/service incident reporting or security vetting requirements, building lawful interception capabilities, data retention regimes, privacy and reshoring requirements or cybersecurity and reporting obligations.

Having due regard to Member States' sovereignty as well as to security issues, it is worth reflecting on whether and how those other barriers could be addressed to allow achieving scale and enhance innovation. For example, in relation to security incidents or security vetting in order to improve harmonisation and a high level of security, different measures could be envisaged, such as introducing close cooperation between those Member States where a core network spans, guaranteeing core network operators the right to request all competent authorities of the Member States in which they provide networks to agree on a set of conditions and requirements to be consistently applied throughout the network and be verified at a one stop shop; defining security requirements for core network operators through EU level guidance etc. As regards law enforcement obligations such as lawful interception, one option could be that core network operators identify in each Member State where they operate a point of contact for competent national law enforcement authorities. Soft law measures, such as an EU recommendation or guidelines, could help identify and specify such solutions on security and law enforcement.

3.2.5. Radio spectrum

Spectrum plays a pivotal role in wireless connectivity and should be managed in the best coordinated way possible among all Member States to fulfil the Union objectives of sustainable development, balanced economic growth, economic, social and territorial cohesion, and solidarity among Member States. Earlier attempts to establish greater EU coordination in spectrum management were not fully successful, and, in parallel, discrepancies and delays have been observed in authorising spectrum for 5G deployment across the Member States. As a consequence, Europe is lagging today behind its international competitors on uptake of 5G.

The observations in Section 2 indicate that there is scope to further improve and make spectrum management fit for the Digital Decade needs and targets.

3.2.5.1. Adapting spectrum management to Digital Decade needs: lessons learned from earlier legislative efforts

A number of proposals by the European Commission to harmonise better the release and licensing of radio spectrum for mobile services have faced considerable resistance in the past 10 years. In view of the delays, fragmentation and artificial scarcity that led to very high prices paid for spectrum it is worth considering whether solutions that were proposed in earlier legislative efforts, but eventually not passed by the co-legislators, could have avoided some of the negative effects that are now evident given the delayed 5G deployment. Considering the necessity of completion of 5G roll-out and timely 6G deployment, more cooperative approach between the national and European level is of vital importance for EU competitiveness. In this context, areas that deserve to be considered and possibly lead to relevant actions include:

- EU level planning of sufficient spectrum for future use cases,
- strengthening EU level coordination of auction timing and authorisation of new spectrum bands,
- considering more uniform criteria for auctions as well as a mechanism similar to the one set by Article 32 of the Code for the coordination of authorisation procedures and conditions regarding the use of spectrum in the internal market.

No wireless service can be deployed without the availability of sufficient spectrum resources. This would include evolving and new areas such as vertical use cases, 6G, IoT applications, WiFi, local spectrum use as well as rapidly developing satellite communication applications such as secure government or commercial ones based on direct device-to-satellite connectivity. In this context it should be considered whether, to ensure new technology advancements are rolled out across the EU at the same time, a 6G roadmap should be enshrined in the law and enforced in a coordinated way by all Member States.

Coordinated release and refarming of spectrum would be crucial in this context. Key example is the coordinated switch-off of 2G and 3G networks (with release of the relevant spectrum for other uses) while, in parallel, implementing solutions for continuous support of important legacy services such as emergency communications.

At the same time, efficiency in spectrum use should be further enhanced to meet the fast growing needs of existing and future wireless applications. For example, stricter conditions attached to spectrum usage rights could be considered, where appropriate, including the principle of ‘use it or lose it’ so as to avoid the creation of barriers to market entry and inefficient allocation of scarce resources. Efficiency could also be achieved whenever possible through shared and flexible use of spectrum with innovative and dynamic solutions or new forms of licensing and methods using, for example, databases and licensed-shared access, geolocation, artificial intelligence and cognitive radio technologies. Parallel to enabling new services, spectrum efficiency can significantly enhance consumer experience, quality of service, competitiveness, and environmental sustainability.

Moreover, looking at the deployment of the next wireless communications technologies, Europe cannot afford yet another spectrum authorisation process spreading over almost a decade, with huge disparities in timelines of auctions and network infrastructure deployment

between Member States. To avoid that the same problems appear in the future it should be considered to better coordinate timing of auctions and ensure it is tighter across the whole EU.

The Single Market could benefit from better coordinated selection criteria and usage conditions and rights for spectrum including their appropriate duration to promote efficient investment across the whole EU. In this context, to date, the voluntary spectrum authorisation peer review mechanism that was adopted under the Code has not proven to be efficient. Therefore, as an alternative a notification mechanism for market analysis as implemented under Article 32 of the Code could be considered.[55]

3.2.5.2. New challenges in spectrum management

In the context of the reflection on core networks (discussed in 3.2.4), it is worth exploring the possibility, on the spectrum management side, to request to competent authorities for operators of EU core networks or pluri-national licensees to seek better aligned national authorisation processes and conditions so as to increase their communications capacities. This could primarily apply with regard to the existing spectrum usage rights or general authorisations, notably with regard, in particular, to the duration of licenses, or spectrum usage conditions such as quality of service objectives/obligations in the context of the 2030 connectivity targets. These could be aligned to allow pan-EU or plurinational operators to operate in a more harmonised environment across borders. It could take the form of an alignment conciliation procedure which could increase efficiency and ensure legal certainty.

In addition, the fast development of the satellite sector and its cross-border nature invite new reflections regarding enhanced or common licensing regimes (even EU-level coordinated spectrum selection and authorisation, if appropriate, to promote the emergence of cross-border or genuine pan-EU operators, while leaving spectrum revenues to the Member States.

Spectrum efficiency and investment incentives should be considered a priority, alongside competition considerations, in market shaping measures for example as regards reservation for new entrants or spectrum caps and overall design of auction processes. In this respect, it should be noted that, while auction prices for 3G and 4G were even higher[56], 5G auctions implemented in the Europe between 2015 and 2023 still raised around EUR 26 billion, not to mention the administrative charges due to national authorities for spectrum management. This amount was paid by operators, in addition to the investments necessary for the deployment of the network infrastructure. The consequence thereof (particularly in cases of artificial increase of the spectrum price without adequate market justification) has been roll-out delays and suboptimal network quality and performance to the detriment of consumers and businesses. To help bridge the significant investment gap in the deployment of advanced communications networks, the financial burden could be alleviated by adopting bidding processes geared towards infrastructure investments.

Considering the potentially enlarged scope of the tasks that will need to be developed at EU level regarding radio spectrum, in particular with regard to coordinated, harmonised or common selections or authorisations, a more integrated spectrum governance mechanism at EU level should be considered. From an international perspective, a more coherent spectrum

[55] Differences in the auction design and timing, as well as spectrum reservations created a diverse -landscape in the EU for the advancement of 5G.

[56] More than EUR 100 bn for 3G and EUR 40bn for 4G.

management approach should be developed to ensure the EU's digital sovereignty and to defend EU interests at international level.

In this regard, the EU should retain full control over EU spectrum decisions especially when confronted with geopolitical and security challenges to guarantee the cybersecurity, independence and integrity of EU communications networks. This includes, in particular, the preparation of technical harmonisation measures for the use of spectrum in the Union[57] and of international negotiations such as World Radiocommunication Conferences. Member States, if appropriate at Council level, should be able to take positions regarding spectrum management in full independence. This means reconsidering the role of the European Conference of Postal and Telecommunications Administrations (CEPT) in EU decision making, given the representation of non-EU Member States in this international body. Going forward, while continuing to rely on the technical expertise of CEPT, the Commission could be assisted by an ad hoc group composed solely of the Member States' representatives whenever EU sovereignty issues might be at stake.

EU and Member States' interests should also be defended at the EU external borders and globally through common actions adopted by all Member States and the EU in full spirit of solidarity. Harmful radio interference affecting Member States and originating in third countries should therefore be addressed through strong and efficient action not only by the Commission but also, by all Member States acting jointly, which is not currently the case, in support of bilateral negotiations and in multilateral negotiations with third countries including in international fora such as the International Telecommunication Union.

Better alignment of existing and future spectrum usage rights, clarity in the policy orientations for the coming decade and more certainty in spectrum management throughout the Union could promote investments and boost EU competitiveness and scale, eliminate remaining barriers caused by the fragmentation induced by national practices for the achievement of the internal market of converging high-speed wireless broadband communications and enable planning and provision of integrated multi-territorial networks and services and economies of scale, thereby fostering innovation, economic growth and the long-term benefit of end users.

3.2.6. Copper switch-off

The migration from legacy copper to newly deployed fibre networks is a key process to facilitate the transition towards the new connectivity ecosystem and contributes to the EU's green objectives. At the same time, it will promote the take-up of the new services and thus contribute to increasing the return on fibre investment and support the achievement of the Digital Decade target whereby, by 2030, all end users at a fixed location should be covered by a gigabit network up to the network termination point.[58] While the decommissioning of copper networks has the potential to decrease the OPEX costs for operators providing at the same time a more sustainable infrastructure due to lower energy consumption, the process requires coordination of all stakeholders. Predictable and balanced measures are necessary to avoid the migration reversing competitive gains, including competitive infrastructure roll-out, under the current

[57] Under the 676/2002/EC Radio Spectrum Decision, with a view to the adoption of technical harmonisation measures to ensure the availability and efficient use of radio spectrum, the Commission is cooperating with the CEPT gathering experts from national authorities responsible for radio spectrum management from 46 European countries, including the 27 EU Member States.

[58] Another possible scenario is that copper networks would be at least partially replaced by fixed wireless access products (based on 5G). Moreover, significant differences in fibre deployment pace may lead to smaller, localized markets, not allowing a truly single market to emerge.

regulatory regime. The needs of end-users, in particular vulnerable groups and end-users with disabilities, should also be carefully addressed. While the Code already contains provisions on migration processes and the new Gigabit Recommendation[59] aims at providing updated guidance to regulators, a clear path towards migration would send a strong signal to the sector further incentivizing investment.

Currently, the process of copper switch-off varies considerably in the EU. By 2023 the leading fixed line operators have announced plans for switching off their copper network in 16 Member States[60], while actual decommissioning has already commenced in 10 Member States.[61] However, the progress within these Member States varies significantly.[62]

The copper switch-off process requires close monitoring. NRAs should ensure that the design of the switch-off process by the operator with significant market power (SMP), in particular as regards its timing and agenda, does not allow strategic behaviour that would risk weakening competition at wholesale or retail level. Some operators, at least initially, would not switch off copper (in particular if it is supplemented by vectoring which enables higher quality of broadband services). It cannot be excluded that some operators would rather switch over customers from copper to fibre via lock-in strategies that would undermine the business case of FTTH alternative operators. Operators would lower wholesale prices in view of FTTH entry in order to keep wholesale customers. Therefore, the regulatory incentives for the switch off, in particular on temporary copper price increase during the switch-off phase as proposed in the Gigabit Recommendation, should be accompanied by sufficient safeguards to preserve competition (similar to those agreed under the GIA and described in next section). Furthermore, lighter access regulation on very high capacity networks could be imposed by applying pricing flexibility, subject to safeguard mechanisms as provided in the new Gigabit Recommendation.

In light of above, setting a recommended date for achieving the copper switch-off would provide for planning certainty throughout the Union and would offer all end-users opportunities of fibre connections under similar timeframe. Considering the national circumstances and the connectivity targets set in the Digital Decade, achieving a copper switch-off for most [XX%] subscribers in the EU by 2028 and the remaining last [1-10%] by 2030 seems appropriate. Such a clear roadmap for copper switch-off would support the 2030 connectivity targets and send a strong signal for investors that there is a clear path towards a return on investment in fibre networks.

3.2.7. Access policy in a full fibre environment

In the 90s and early 2000s, the objective of liberalisation of the EU electronic communications sector was, following the global trends, to bring competition into a sector characterised by legal/statutory monopoly and to combat historical negative consequences of such monopoly (e.g. inefficiency, lack of innovation, low quality, monopoly rents). However, from its very inception, the ultimate goal was to limit sector specific regulation over time and - after a

[59] Commission Recommendation of 6.2.2024 on the regulatory promotion of gigabit connectivity, C(2024) 523 final.

[60] BE, EE, EL, ES, FI, FR, HU, IE, IT, LU, MT, PL, PT, SE, SI, SK.

[61] BE, EE, ES, FI, LU, MT, PL, PT, SE, SI.

[62] See also BEREC summary report on the outcomes of the internal workshop on the migration from legacy infrastructures to fibre-based networks, 5 Dec. 2019, BoR (19) 236.

transition period and subject to competition developments - to migrate in the sector to a market-based environment subject only to competition rules[63].

Ex-ante regulatory intervention has been successful in lifting barriers to competition in the national market for fixed legacy networks. The emergence of competition after regulatory intervention made it possible to reduce the number of markets that national regulators need to assess ex-ante from 18 to 2 between 2003 and 2020[64]. As the markets subject to ex-ante regulation and the number of operators designated as having SMP diminish in view of progressing deployment of competing network infrastructures, the question is whether it is the right time to explore the possibility of not recommending at the EU level any markets for ex-ante regulation. The possibility of leaving electronic communications networks to ex-post control only appears to have merit, as in many densely populated areas end customers already now benefit from a choice of at least two independent broadband networks (e.g. coaxial cable and fibre), while in some other areas electronic communications operators transformed themselves into functionally separated or wholesale only entities.

Despite this progress, some barriers still persist (and may continue to persist in near future) in some geographical areas (in particular rural/remote), and the need for ex ante intervention in such cases remains. However, with the objective to foster the progressive deployment of alternative fibre networks and with legacy networks of former incumbents to be ultimately replaced by Gigabit networks, the Commission and the NRAs will need to further adjust their intervention to keep pace with the market evolution and ensure investment incentives which are reduced by the prospective of overbuilding. In particular, NRAs should monitor the observed variations in competitive conditions, particularly the degree of infrastructure competition, at the stage of market definition, potentially defining separate geographic markets and limiting ex ante regulation to the areas where it is still needed. In cases where NRAs consider that the boundaries of geographic areas with different competitive conditions would not be stable, they should apply differentiated remedies, ensuring their appropriateness and proportionality[65].

To foster pan-European network roll out, the development of a more EU-level access regulation toolkit could be envisaged to complement or replace, when necessary, the national/local approach. Indeed, in a full-fibre environment, access products can be provided more centrally and at the higher network level without undermining the capacity of access seekers to compete in terms of the services and quality as offered to the end users. Such EU-wide remedies already exist in the current framework and they have very been successful in tackling common issues across the EU (e.g. introduction of single Union-wide mobile termination rates or roaming). They led to less burdensome albeit effective regulation reducing fragmentation. Already the 2013 "Connected Continent" proposal[66] envisaged a set of harmonised access remedies. A decade later, the lack of cross-border consolidation of telecommunications markets persists. Therefore, time appears ripe for considering the introduction some EU-wide access remedies.

---

63 Recital 29 of the Code states: *"This Directive aims to progressively reduce ex ante sector-specific rules as competition in the markets develops and, ultimately, to ensure that electronic communications are governed only by competition law"*

64 Commission Recommendation (EU) 2020/2245 of 18 December 2020 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with the Code (the 2020 Recommendation on Relevant Markets) (OJ L 439, 29.12.2020, p. 23-31).

65 See recital 172 of the Code.

66 Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012 (COM/2013/0627 final - 2013/0309 (COD))

While broadband access networks will remain predominantly of local character (due to demand and supply patterns), such unified and standardised access product could in turn facilitate the further integration of the single market.

Furthermore, under the provisional agreement on the Gigabit Infrastructure Act[67], which introduces symmetric regulation for access to civil engineering assets, there are specific provisions aimed at protecting the business case of FTTH operators (although in some cases optional for Member States to implement[68]). Operators investing in new fibre networks will be able to refuse access to their (newly deployed) physical infrastructure if they provide passive wholesale access, such as dark fibre or fibre unbundling, suitable for the provision of very high capacity networks under fair and reasonable terms and conditions. Such a protection will be even reinforced in the case of networks deployed by public sector bodies in rural or remote areas. There any network operator (e.g. an utility company) or a public sector body (and not only the same operator receiving the access request) could refuse access to physical infrastructure if a passive wholesale access product can be offered by the operator of a network, operated on a wholesale only basis, owned or controlled by a public sector body. At the same time, while phasing out ex ante regulation to foster investments incentives for the deployment of physical fibre networks across the whole of the EU, competition can be still preserved by providing for virtual access also in new forms allowed by the undergoing technology changes, such as network slicing. Such type of access could also lower the barriers to rolling out pan-European networks on a virtual basis.

Finally, where symmetric and harmonized regulation offered by standard remedies would not be sufficient and market failures would still persist, a safety net allowing continued ex-ante local regulation could be maintained. For this purpose, the "3 Criteria Test"[69] should allow NRAs to determine (sub-national) markets where ex ante regulation is still necessary to address persistent market failures. In such (limited) geographic areas the SMP regulation could ensure that local access seekers remain in the market and prevent re-monopolisation of less densely populated areas or more in general in absence of competitive pressures. The limited SMP-based regulation could be ancillary or replaced to more general, harmonised symmetric rules addressing access to civil engineering infrastructure with safeguards providing investment certainty, e.g. in view of risk of unreasonable overbuild.

---

67 [reference to the press release on the political agreement].

68 Member States could allow network operators and public sector bodies to refuse access to physical infrastructure by offering active access, such as bitstream as an alternative to physical access, under conditions, i.e. the deployment project of the requesting operator addresses the same coverage area, there is no other fibre network connecting end-user premises (FTTP) serving this coverage area, and the same or an equivalent refusal possibility is applied at the date of the entry into force of the regulation, in the Member State in accordance with national law complying with Union law. Also, networks deployed by undertakings owned or controlled by public sector bodies in rural or remote areas and operated on a wholesale only basis could receive an extra protection from competition if a Member State allows them to refuse requests to coordinate civil works.

69 In accordance with Article 67(1) of the Code and Recital 22 of the 2020 Recommendation on Relevant Markets, the national regulatory authorities can also define other relevant product and service markets, not recommended for ex-ante regulation, if they can prove that in their national context, the markets meet the three criteria test. A market may be considered to justify the imposition of regulatory obligations if all of the following criteria are met: (a) high and non-transitory structural, legal or regulatory barriers to entry are present; (b) there is a market structure which does not tend towards effective competition within the relevant time horizon, having regard to the state of infrastructure-based competition and other sources of competition behind the barriers to entry; (c) competition law alone is insufficient to adequately address the identified market failure(s).

3.2.8. [70]Universal service and affordability of digital infrastructure

The availability of adequate broadband internet services, of the quality that is needed to perform basic tasks on-line, such as eGovernment services, social media, browsing or performing video calls, is ubiquitous throughout the EU. Hence, in most of the Member States, Universal Service obligations are focused on consumers with low income or special needs.

However, in the future, a different kind of social exclusion may emerge, that of weaker end-users not being able to benefit from the best available networks due to their localisation (for example rural/remote areas) or due to the price of services. It is important to ensure that this does not lead to a social digital divide, and that all end-users, may reap the benefits of very-high speed connectivity. It is hence important to ensure that Member States take measures to support weaker end-users.

The importance of ensuring Universal Service in the future has also been acknowledged by the European Parliament, the Council and the European Commission in the "European Declaration on Digital Rights and Principles for the Digital Decade". According to its principle 3 "*Everyone, everywhere in the EU, should have access to affordable and high-speed digital connectivity"* and they commit to "[…] *ensuring access to high-quality connectivity, with available Internet access, for everyone wherever in the EU, including for those with low income".*

Sector-specific universal service obligations have relied on two modes of financing: state financing and sector financing, the latter being the predominant form. Sector financing has so far been limited to electronic communications providers, while providers of NIICS have been excluded. In this respect, some respondents to the exploratory consultation were of the view that Universal Service obligations should evolve to meet the future connectivity demands.

In addition to the Universal Service, a number of Member States have tried to ensure the affordability of networks through state financing in the form of connectivity vouchers with the view to boosting the take-up of high-speed offers. The latest Broadband State Aid Guidelines have clarified the conditions under which such connectivity vouchers may comply with EU State aid rules and the General Block Exemption Regulation exempts now from notification certain types. Vouchers, financed by the Member States, may be used to prevent or remedy any divide in access to very high -capacity networks.

3.2.9. Sustainability

A focus on environmental sustainability aspects of the digital transformation of the economy and society is a key requirement of the Digital Decade Policy Programme. The recent COP28 drew on EU proposals and actions in the field and launched a Green Digital Action in an effort to reinforce the role of digital in reaching international goals on climate change (such as on global warming, e-waste, fossil fuels) with a key involvement of the mobile electronic communications and satellite industry sectors. These developments reinforce and give an international dimension to European efforts in integrating sustainability in digital standards by design.

Another important aspect is to create more awareness on the issue of sustainability in digital networks. In this respect, in its Communication "*Shaping Europe's digital future*"[71] the Commission raised the possibility of introducing 'transparency measures for electronic

[71] COM(2020) 67 final.
[71] COM(2020) 67 final.

communications operators on their environmental footprint' at EU level. The Commission further announced[72] that it will work, in consultation with the scientific community and stakeholders, towards defining common EU indicators for measuring the environmental footprint of electronic communications services and to develop, by 2025, an EU Code of Conduct for the sustainability of electronic communications networks to help steering investments towards sustainable infrastructures. [The results of the work on the sustainability indicators are published in the coming weeks.]

Beyond pursuing sustainability public policy objectives, such transparency efforts could be the basis to create incentives to attract investments in the electronic communications sector to make ICT greener ('green ICT') and have it enable the greening of other sectors ('ICT for green'), particularly where investment funds are increasingly directing funds to green and sustainable infrastructures. The Commission will work with the industry to facilitate the application of the EU taxonomy for green investment in electronic communications networks based on robust and credible metrics.

Nonetheless, to ensure success in achieving sustainability objectives, it is essential that all players of the digital network ecosystem, including CAPs, cooperate towards an efficient use of resources. Beyond concrete actions to reduce carbon footprint, these players could also contribute to increasing transparency on the emissions related to the usage of their services, such as labels informing consumers of the different environmental impact of video resolution settings.

3.2.10. Summary of possible scenarios

- *Scenario 4: In order to address the converged electronic communications connectivity and services sector and to ensure that its benefits will reach all end-users, the Commission may consider the broadening of the scope and objectives of the current regulatory framework to ensure a regulatory level playing field and equivalent rights and obligations for all actors and end-users of digital networks; given the likely global magnitude and impact of the technological developments and of any possible regulatory changes, a reform of the current framework needs to be debated broadly with all stakeholders;*

- *Scenario 5: In order to address technological and market developments and the resulting need to change the regulatory paradigm and ensure less burden for companies and more efficient service delivery, while continuing protecting vulnerable end-users, the Commission may consider:*

    - *accelerating copper switch-off (fixed deadline 2030 and support for switch-over from 2028).*

    - *a change to access policy in view of full fibre environment, by proposing a European wholesale access product and recommending no markets for presumptive ex ante regulation while maintaining a safety net for NRAs to keep regulation if the "3 Criteria Test" is met (reverse burden of proof). In the alternative, only markets for civil infrastructure might be considered for regulation ex ante (as the most persistent bottleneck), combined with the*

[72] COM(2022) 552 final.

implementation of lighter access regulation (no price regulation or pricing flexibility) along the lines of the Gigabit Recommendation

- *Scenario 6: In order to facilitate the single market and building scale for activities of all players, the Commission may consider:*
    - *a more integrated governance structure at Union level for spectrum that would allow, where necessary, for greater harmonisation of spectrum authorisation processes and enhance Union's sovereignty in spectrum management; the Commission may also consider solutions for more aligned authorisation and selection conditions, or even single selection or authorisation processes, for terrestrial and satellite communications and other innovative applications that make clear cases for fostering the development of the single market;*
    - *a more harmonized approach to authorisation (through the possible establishment of "country of origin" principle)*
- *Scenario 7: The Commission may consider facilitating greening of digital networks through the switch-off of copper and the move to full fibre environment and a more efficient use of networks (codecs)*

3.3. Pillar III: Secure and resilient digital infrastructures for Europe

To protect the value of the massive investments that Europe is to undertake to build the cutting-edge infrastructure that it needs to deliver economic growth and societal benefits, it is important to ensure that such infrastructure is secure. Given the threats outline din Section 2 above, adequate attention should be given to both physical security, notably in relation to the backbone infrastructure, as well as to the transmission of data from end to end of the network.

3.3.1. Towards secure communication using quantum and post-quantum technologies

Advances in quantum computing come with implications for existing encryption methods, which play a crucial role in ensuring end-to-end security in digital networks, including telecommunication networks and the critical infrastructures they are underpinning. Although quantum computers capable of breaking current encryption algorithms are not yet a reality, the first operational quantum computers are being deployed world-wide. Therefore, the EU needs to anticipate the maturing of quantum computers and start developing transition strategies towards a quantum-safe digital infrastructure now, i.e. secure against attacks from quantum computers. Short of this, the effort and investment in cutting-edge digital infrastructure to deliver applications of critical societal relevance, such as in the field of mobility or healthcare, could be compromised.

Post-Quantum Cryptography (PQC) is a promising approach to make our communications and data resistant to quantum attacks, as it is based on mathematical problems hard to solve even by quantum computers. As a software-based solution, for which new dedicated hardware is not necessary, PQC allows for a swift transition to higher protection levels.

PQC is already high on the agenda of many countries. National authorities, like the *Agence nationale de la sécurité des systèmes d'information* (ANSSI) in France, or the *Bundesamt für Sicherheit in der Informationstechnik* (BSI) in Germany, as well as the European Union Agency

for Cybersecurity (ENISA) have published reports on preparing for the implementation and deployment of PQC.[73] The US Cybersecurity and Infrastructure Security Agency (CISA) established a PQC Initiative to unify and drive agency efforts to address threats posed by quantum computing.[74]

However, the current framework in the Union cannot fully address the challenges posed by the migration to a quantum-safe digital infrastructure. Addressing these challenges requires a coordinated effort at EU level, involving mainly government agencies. For an effective transition towards PQC, efforts should be synchronized ensuring the roadmaps are aligned at Union level, with concrete timelines for every transition step. Assessment of the implementation of the transition plans will be beneficial not only to gather information on practical challenges and gaps, but also for anticipating needs for future EU regulatory requirements.

3.3.2. Way forward

In this regard, it is important to encourage Member States to develop a coordinated and harmonized approach, ensuring consistency in the development and adoption of EU PQC standards across Member States. This consistency would promote interoperability, allowing systems and services to function seamlessly across borders, preventing fragmentation different levels of efficiencies in the transition, and ensures a European approach to PQC. Measurable effects of the transition are expected to appear around 2030. This step appears to be compelling and needed to preserve future policy options in an evolving technology landscape. That is why the Commission sets out recommendations to this effect together with this White Paper.

In the long-term, Quantum Key Distribution[75] (QKD), will offer additional security to our communications, at the physical network layer. Hybrid implementation schemes PQC/QKD are part of guidelines issued by different National Security Agencies and enter discussions about the design of coordinated actions at EU level. The combination of QKD and PQC will allow for full end-to-end security in our digital communications. QKD represents a hardware-based solution which is based on the unique properties of quantum physics, rather than on mathematical functions, and it is in principle inherently robust against brute-force attacks, as well as against new mathematical discoveries that are the underlying weakness of classical cryptography. Intense research is ongoing on different fronts to overcome the current practical challenges of this technology, and first deployment test-beds are at present being delivered under the EuroQCI initiative[76] funded by the DEP. In principle, QKD will represent a full paradigmatic shift of the digital infrastructure ecosystem, and constitutes already now a forward-looking, highly competitive technology of high interest also for future applications such as the Quantum Internet.

---

[73] ANSSI Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie post-quantique anssi-avis-migration-vers-la-cryptographie-post-quantique.pdf ; BSI. Migration zu Post-Quanten-Kryptografie. Migration zu Post-Quanten-Kryptografie - Handlungsempfehlungen des BSI (bund.de) ; Post-Quantum Cryptography: Current state and quantum mitigation — ENISA (europa.eu) ; Post-Quantum Cryptography - Integration study — ENISA (europa.eu)

[74] https://www.cisa.gov/news-events/news/cisa-announces-post-quantum-cryptography-initiative

[75] The Commission is working with all 27 EU Member States, and the European Space Agency (ESA), to design, develop and deploy the European Quantum Communication Infrastructure (EuroQCI). It will be an integral part of IRIS², the new EU space-based secure communication system.

[76] The European Quantum Communication Infrastructure (EuroQCI) Initiative | Shaping Europe's digital future (europa.eu)

3.3.3. Towards security and resilience of submarine cable infrastructures

As described in Section 2.4 above, the security and resilience of the EU's network and computing infrastructure is an essential element of our digital autonomy. In particular, it is clear that submarine connectivity and submarine cables are a particularly pressing issue of EU sovereignty and pose a challenge to EU resilience. EU legislation provides for the security of submarine cables where these are used in particular by providers of public electronic communications networks or services. The Code requires providers of such services to take appropriate and proportionate technical and organisational measures to manage appropriately the risks posed to the security of networks and services, including the protection from physical and environmental threats.

From October 2024, these provisions will be replaced by the more ambitious provisions of the NIS 2 Directive. Under the new Directive, Member States are required to adopt policies related to sustaining the general availability, integrity and confidentiality of the public core of the open Internet, including, where relevant, the cybersecurity of critical infrastructure including submarine communications cables. Member States should further ensure that the security of the communication networks is maintained and that their vital security interests are protected from sabotage and espionage. In addition, the NIS 2 Directive applies the same principles to other entities that might also operate submarine cables, such as providers of cloud or data centre services. Given that international connectivity supports and accelerates the digitalisation and competitiveness of the EU, any incidents affecting submarine communication cables should be reported to the relevant National Computer Security Incident Response Team or competent authority. The national cybersecurity strategy of Member States should, when relevant, take into account the cybersecurity of submarine communications cables and include a mapping of potential cybersecurity risks and mitigation measures to secure the highest level of their protection.

In February 2023, NATO established a Critical Undersea Infrastructure Protection Cell (CUIPC) to address the security of inter alia submarine cables. In the context of the EU-NATO Taskforce on the resilience of critical infrastructure cooperation, it was recommended to jointly "*[e]xplore possibilities for exchanges on how to improve the monitoring and protection of critical infrastructure in the maritime domain by relevant authorities and discuss ways to enhance maritime situational awareness*". In meetings between EU and NATO officials, several Member States and other allies have highlighted the need to ensure structured cooperation between the new NATO CUIPC and relevant EU entities. Despite these efforts, incidents such as in the Baltic Sea, following which Finland activated the EU Hybrid Toolbox mechanism,[77] have demonstrated the EU's vulnerability and underline the need to advance and coordinate work at EU level to foster cable security and resilience. The European Council on 27 October 2023 consequently stressed "*the need for effective measures to strengthen the resilience and ensure the security of critical infrastructure"*, while underlining *"the importance of a comprehensive and coordinated approach*."

As mandated by the Council Recommendation on resilience of critical infrastructure concerning submarine cable infrastructure, the Commission carried out studies and consulted relevant stakeholders and experts on appropriate measures in relation to possible significant incidents regarding submarine infrastructures. The non-confidential parts of the study will be shared with Member States at the appropriate information security level.

[77] Council conclusions of 21 June 2022 on a Framework for a coordinated EU response to hybrid campaigns

A key conclusion is that the current framework in the EU cannot fully address the challenges identified above. Concrete elements currently lacking include an accurate mapping of existing cable infrastructures informing a consolidated EU-wide assessment of risks, vulnerabilities and dependencies, a common governance of cable technologies and cable-laying services, ensuring rapid and secure repair and maintenance of cables, as well as the identification and funding of critical intra-EU and global cable projects.

3.3.4. Towards a more centralised governance framework for cables

To overcome the identified challenges and protect the European interests, long-term measures need to be considered. While the exact scope of these measures would need to be defined, a focus area should be the reinforcement of advanced R&I activities to strengthen the economic security of the EU, particularly in support of new fibre and cable technologies as part of the strengthening of the EU's technical capacity as laid out in Section 3.1 above.

Another key area to be addressed in the long term concerns the financing of new strategic submarine cable infrastructures and to increase the security and resilience of existing ones.In this respect, a future amendment of the CEF Regulation could be considered in order to establish a CPEI cable list and related labelling system of strategic Cable Projects of European Interest (CPEIs) that would address identified risks, vulnerabilities and dependencies. CPEIs could be conceived to comply with the most advanced technological standards, such as sensor capabilities for their own monitoring and to support EU policies in the field of security, sustainability, or civil protection.

More generally, it will be important to ensure appropriate funding of CPEIs and the need to pool together funding instruments, such as Structural Funds – with particular attention to NDICI-Global Europe in the context of Global Gateway – as well as EU financing (EIB and exploring the feasibility and potential leverage effect of a financial instrument investing in CPEI and 5G), to ensure synergies and that adequate investments are injected in CPEIs, updating procurement rules where required. This could potentially and progressively take the form of an equity instrument, supporting by design such CPEIs. Member States could decide to support CPEIs via the IPCEI framework or other contributions in compliance with EU State aid rules.

As a result, a joint EU governance system on submarine cable infrastructures could be envisaged, including: (i) additional elements to consider for mitigating and addressing risks, vulnerabilities and dependencies under a consolidated EU-wide assessment, and priorities for increasing resilience; (ii) revised criteria to upgrade existing or to fund new cables; (iii) an update of the co-created priority list of CPEI, both intra-EU and international, based on strategic importance and respect for the above criteria; (iv) pooled funding from various sources for such projects, including through equity funds in which the Union could participate with Member States to de-risk private investment and (v) further actions to secure supply chains and avoid dependency on high-risk third-country suppliers.

Point (iv) could include specific action regarding the reinforcement of maintenance and repair capacity at EU level, which would mitigate the impact of any attempts to sabotage submarine cable infrastructure. This work stream could learn from the experience gained under the Union Civil Protection Mechanism and RescEU, particularly regarding firefighting, with a view to building up an EU-funded fleet of maintenance and repair vessels.

Finally, the need to work towards harmonised security requirements should also be addressed and promoted in international fora, including through the identification of best-in-class

standards that harness the latest developments in security and self-monitoring capacities for cables and associated routing and relay equipment, which could be recognised through a dedicated EU certification scheme.

To safeguard the space for future policy options in the current geopolitical context described above, alongside this White Paper, the Commission recommends to Member States certain immediate actions to prepare measures in the longer term. In the Recommendation the Commission specifies possible actions specifically related to submarine cable infrastructure that Member States can adopt in the implementation of the Council Recommendation on resilience of critical infrastructure concerning submarine cable infrastructure. The Commission Recommendation will ensure that Member States and the Commission work together to implement a coordinated and robust approach as a precursor to the identification of the likely needs for increased EU funding of relevant R&I activities and eventually a more centralised governance framework in the longer term.

3.3.5. Summary of possible scenarios

- *Scenario 8: The Commission will aim at reinforcing advanced R&I activities in support of new fibre and cable technologies.*

- *Scenario 9: The Commission may consider an amendment of the Connecting Europe Facility Regulation in order to establish a CPEI labelling system.*

- *Scenario 10: The Commission may consider an equity instrument designed to support CPEIs.*

- *Scenario 11: The Commission may consider implementing a joint EU governance system on submarine cable infrastructures.*

- *Scenario 12: The Commission will aim at harmonising security requirements in international fora, which may be recognised through a dedicated EU certification scheme.*

4. CONCLUSION

As we are at the crossroads of major technological and regulatory developments, it is of tantamount importance to debate these developments broadly with all stakeholders and like-minded partners. Hence, with this White Paper the Commission launches a broad consultation of Member States, civil society, industry, and academics, to collect their views on the scenarios outlined in this White Paper and provide them with an opportunity to contribute to the Commission's future proposals in this domain.

These proposals include both policy means to ensure secure and resilient digital infrastructures and possible scenarios for key elements of a future regulatory framework. This consultation will allow a comprehensive dialogue with all concerned parties that will inform the next steps of the Commission.

The Commission invites comments on the proposals set out in the White Paper through an open public consultation available at https://ec.europa.eu/info/consultations_en. The consultation is open for comments until [XX.YY.2024].

It is standard practice for the Commission to publish submissions received in response to a public consultation. However, it is possible to request that submissions, or parts thereof, remain confidential. Should this be the case, please indicate clearly on the front page of your submission that it should not be made public and also send a non-confidential version of your submission to the Commission for publication.