CENTRAL EUROPEAN LAWYERS INITIATIVE

QUICK ANALYSIS

EU Commission's White Paper on digital infrastructure transition

The Commission's White Paper published on 22 February proposes the implementation of new public policy measures, including the potential introduction of a Digital Networks Act, all to encourage the further development of digital networks, oversee the shift to new technologies and novel commercial strategies. Such policies should not, requires the Commission, fall short of catering the connectivity requirements of all users and safeguarding the security of infrastructures for the economic security of the Union.

I. Introduction

The White Paper (CWP) underscores the crucial importance of advanced digital network infrastructures for the security and overall competitiveness within the European Union. It picks up the thread from the EU's Digital Decade Policy Programme 2030, and places emphasis on the significance of secure and sustainable digital infrastructures as fundamental for enabling transformative technologies like Artificial Intelligence (AI), Internet of Things (IoT), and smart grids. These technologies play a significant role in driving GDP growth and facilitating the digital and green transition in the European Union (EU). In the following we look at the paper's Pandora's box.

II. Main challenges in the Digital Infrastructural sector

The new convergence: cloud and network

The emergence of service platforms is noted as a significant development, enabling non-traditional entities such as cloud hyperscalers to enter the network services sector. Now, considers the CWP, the distinction between *electronic communications providers* and *digital service providers* is becoming less relevant, leading to the creation of a multifaceted ecosystem.

The most significant "convergence wave" that impacted the telecommunications industry took place in the early 2000s, leading to the establishment of the revised but still existing European regulatory framework for the industry. That convergence was primarily driven by digitization, which facilitated the transmission of data, voice, and audiovisual signals over a unified network. Now the convergence that we are witnessing allows for the deployment of *specific network infrastructure components* (such as firewall equipment and DDoS systems) in the cloud, establishing the *network-as-a-service business model*. This model is rooted in the regulated traditional telecommunications infrastructure, while cloud providers are not subject to the European Electronic Communications Code. Such confrontation between the two ends gave rise to inquiries regarding whether uniform regulatory rules should apply to all

participants in this ecosystem and whether end-users, especially consumers, should possess comparable entitlements. Despite the operation of extensive electronic communications networks by cloud providers, certain aspects of the electronic communications regulatory framework, particularly related to access regulation and dispute resolution, do not apply to these networks. The CWP aims to remedy this problem, too.

Radio spectrum policy

The management of radio spectrum policy within the European Union involves a joint effort by both the EU and its individual Member States. The EU establishes regulations to standardize frequency band allocation, while individual Member States are responsible for authorizing, managing, and utilizing the spectrum. In spite of such long-standing framework, in the absence of cohesive oversight, inconsistencies in the deployment of wireless technologies such as 4G and 5G have occurred. Previous attempts to enhance coordination within the EU in the management of spectrum, such as the regulation on the Single Market for Telecommunications and the Code for European Electronic Communications, have not achieved significant success. 5G was inconsistently deployed, leading to some member states being almost a full generation behind in terms of wireless technology. This prompts inquiries into the effectiveness of different national situations for assigning spectrum, indicating that a more cohesive European strategy might have economic and technical rationale.

The Commission's paper also emphasizes the achievements of information society services, which have experienced rapid growth through the application of the 'country of origin' principle. This principle allows service providers to adhere to the regulations of their originating Member State instead of having to comply with the regulations of every Member State in which they conduct operations. The CWP proposes coordinated actions, such as the *simultaneous deactivation of 2G and 3G networks*, in order to free up spectrum for advanced technologies, while also ensuring continued support for important existing services.

Submarine cables

The CWP highlights the importance of secure and resilient communication pathways, particularly submarine cables, e.g., for transcontinental data transmission. The EU has been advocating for improved security and durability of submarine cable infrastructures, highlighting the need for *increased public funding alongside private investment*. The Commission's document also identifies key deficiencies in the current regulatory framework, including the lack of *comprehensive delineation of cable infrastructures*, *integrated risk evalua*tion, standardized governance, and recognition and *financing of critical cable initiatives* within the EU and globally.

III. TRANSITION TO THE DIGITAL NETWORKS

Pillar I.: Connected Collaborative Computing" Network ("3C Network")

The CWP emphasizes the importance of efficient digital infrastructures in enabling advanced applications like telemedicine, smart buildings, and business optimizations. It discusses the evolution of on-device edge technology, which empowers various devices with substantial computing power, including AI processors. The main objective, as presented by the CWP, is to establish a resilient "Connected Collaborative Computing" Network ("3C Network") in Europe, encompassing semiconductors, computational capabilities, radio technologies, connectivity infrastructure, data management, and applications, to foster a community of European innovators.

Pillar II: Completing the Digital Single Market

As briefly explained above, the Commission's proposal examines the necessity of reassessing the regulatory framework for electronic communications in light of the convergence of electronic communications networks and cloud services. It is believed that the utilization of applications based on Network as a Service (NaaS) that make use of independent 5G core networks and network slicing has the potential to facilitate the emergence of novel business models for cross-border activities. The CWP, at the same time, acknowledges that technological advancements are decoupling network provisioning from physical proximity and enabling wireless networks, like satellites, to extend coverage beyond national and EU boundaries. This raises questions about the effectiveness of different national circumstances in allocating spectrum and suggests that a more cohesive European strategy may be economically and technically justified.

The document also emphasizes the role of the 'country of origin' principle. This principle entails service providers abiding by the regulations of their home Member State instead of those of every Member State in which they conduct business. According to the document, governments would endorse the advancement of *multinational or European Union-wide telecommunications companies* while ensuring that member states continue to receive income from spectrum usage. The potential implementation of regulatory mechanisms at the EU level is also under consideration to facilitate the deployment of pan-European networks.

Pillar III: Secure and resilient digital infrastructures for Europe

As the development of quantum computers with the potential to break current cryptographic algorithms progresses, there is a call for the EU to establish plans for transitioning to a digital infrastructure that is resistant to quantum threats. One potential

solution, a “post-quantum cryptography” (PQC) was recognized as a crucial strategy for protecting data from quantum attacks, providing a software-oriented remedy that obviates the need for new hardware and facilitates a swift transition to heightened security measures. Over the extended period, it is anticipated that Quantum Key Distribution (QKD) will offer an extra level of security to telecommunications, serving as a supplement to PQC. Quantum Key Distribution (QKD) relies on principles of quantum physics instead of relying on mathematical problems, thus providing a strong defence against potential attacks. The details of this are also subject to further regulatory and policy discussions.

Summary

Main challenges in the digital infrastructure sector include the convergence of cloud and network services, the more innovative and security-based management of radio spectrum policy, and the significance of secure submarine cables for transcontinental data transmission. The discussion paper also highlights the need for a resilient "Connected Collaborative Computing" Network ("3C Network") and the completion of the Digital Single Market to improve connectivity and streamline regulatory frameworks. Additionally, the paper addresses the need for secure and resilient digital infrastructures in the face of quantum threats. We at CELI believe that a great deal of the proposals presented in the paper are in very early stages of development. Market players, national agencies and international organizations must make themselves heard during the consultation period. On our end, indeed, we will be preparing a detailed contribution.