Report of the Broadband Platform Meeting, held on 25 May 2023, Brussels

Ilpo Heltimoinen (FI/ECR) opened the meeting on behalf of the Chair of the ECON Commission, Jaroslava Pokorna Jermanova. He highlighted that digital transformation had become more important than ever. Digital divides continue to be accentuated and we need to make sure that no one will be left behind. This is why the meeting would be focusing on three key topics in particular: **connectivity, digital resilience and assessment of digital maturity of cities and regions**.

I. CONNECTIVITY

Mr Franco Accordino, *Head of Unit for Investment in High Capacity Networks, DG Connect*, provided an overview of the latest advances in the Digital Decade. A high-quality digital infrastructure is an increasingly significant cornerstone of the whole economy, taking its place alongside electricity, gas, water and transport networks. Excellent and secure connectivity for everybody and everywhere in the EU is becoming a prerequisite to deliver sustainable economic and social benefits based on modern online services and fast internet connections. Mr Accordino stressed that the use of fibre and expanding its coverage can improve citizens' lives. Investment in infrastructure is crucial before demand overtakes the services offered. Policy and legislative actions are being taken, including advances such as the Gigabit Infrastructure Act. However, the private sector needs to follow suit, as private investments are further needed to achieve the position to achieve the goals set for 2030. To cover what are called 'market failures', or gaps in the private investment system, 2 billion EUR are being disbursed by the European Union, in projects such as the 5G Cross-border corridors, and in developing best practices, funding projects such as '5G for Smart Communities'. To scale up, more and better practices and services will be provided. He highlighted the importance that better connectivity will have for creating a more inclusive society, and the need for a bottom-up approach. Lastly, he called on the Committee of the Regions to keep working together to achieve this aim.

Silvia Adriana Ticau and **Hannele Lahti** of the *European Commission, DG Connect, Electronic Communications Policy, Implementation and Enforcement Unit* then informed about the Proposal for a Regulation on the Gigabit Infrastructure Act. The current market context can be synthesised in three key points. The first one is the high cost which developing such a level of connectivity presents. It is estimated that over 145 billion EUR are needed to reach 90 per cent of households with FTTH at today's level. Civil works, furthermore, are expected to represent 70 per cent of the total capital expenditure for deployment.

Report of the Broadband Platform Meeting, held on 25 May 2023, Brussels

The second factor that follows is cost, as permit delays can incur costs of 75 million EUR annually, adding 1 to 2 years of delay. However, it is also underlined that coordinating civil works can lead to up to 30 per cent of savings.

The main problems of high deployment costs and persisting slow deployment of networks are mainly driven by absent, incomplete or outdated information on existing physical infrastructure, persisting difficulties in accessing existing physical infrastructure, lack of suitable in-building infrastructure and wiring and challenges in

accessing it, limited civil work coordination, unviable overbuild of Electronic Communications Networks (ECN), procedural complexity, too long and burdensome permits and rights of way processing.

As such, the Gigabit Infrastructure Act has been designed with the following objectives in mind:
- Reducing administrative burden and cost for ECNs: Streamlining permits and limit fees, digitalising permit granting, including better and more information on infrastructure and planned civil works in electronic format, and introducing a single digital interface.
- Accelerating rapid 5G deployment: Developing the possibility of including it in public physical infrastructure, such as public building rooftops.
- Foster fibre deployment: Building new and renovated buildings already pre-equipped with fibre, fibre-readiness and cleaner conditions for access to physical infrastructure.

To achieve this, the Act will be based on four different pillars:

Gigabit Infrastructure Act – what is new?

ACCESS TO PHYSICAL INFRASTRUCTURE
- Widened scope to "operators"
- Public bodies and public assets
- Aspects for determining fair and reasonable
- MSs can exclude certain buildings
- Commission may issue guidance
- Proactive provision of information in electronic format
- New grounds for limitations of transparency

CIVIL WORKS
- Widened scope to "operators"
- Circumstances when a request to coordinate is unreasonable (ECN-ECN)
- Commission may issue guidance
- Proactive provision of information in electronic format with new exceptions

PERMIT GRANTING incl. RoW
- Widened scope to "operators"
- Nationally consistent rules
- Electronic applications via SIP and overall electronic process
- Deadlines for application completeness & 4 months deadline also for RoW
- Tacit approval & "Permit-free" deployments by Commission implementing act
- Fees limited to admin costs

IN-BUILDING PHYSICAL INFRASTRUCTURE
- Fibre-wiring mandated
- MSs establish technical specifications
- Fibre-ready label
- Possibility to combine with certification in energy performance of buildings
- Ground for refusal of access to physical infrastructure
- Commission may issue guidance

The discussion following the presentation focused on identifying the needs and challenges of connectivity (**Michael Murphy (IE/EPP)**, increasing connectivity in rural areas (**Florian Siekmann (DE/Greens)** and the reduction of red tape for connectivity in more isolated areas (**Declan McDonnell (IE/EA)**.

The representatives of the Commission welcomed the insights from CoR Members on the local and regional perspective.

II. DIGITAL RESILIENCE

The other side of the coin to connectivity is <u>cybersecurity and digital resilience</u>. This session started with a presentation of the new ECON study on digital resilience by **Simona Cavallini**, *Senior Researcher* and **Rossella Soldi**, *Managing Director, Progress Consulting*. They first laid out their methodological approach: based on literature review and desk research, studying 8 different case studies in Europe, publishing one online questionnaire, carrying out 10 semi-structured interviews and 2 foresight exercises. For the first time, this study offers a definition of 'digital resilience of public authorities' (Identified as the ability to resist, absorb and recover from disruption through relevant legislation, solid and reliable critical (external + digital) infrastructures and the use of appropriate digital and cybersecurity skills), and the 'Cost of digital non-resilience for a public authority' (The monetary cost needed to restore the functioning and service provision of a public authority affected by a digital incident to a level at least equal to the one existing before the digital incident). Four steps are further

identified for achieving digital resilience: Achievement of political awareness on the relevance of digital resilience; Definition of the most feasible governance model for digital resilience; Choice of investment strategy and identification of funding sources; and digital resilience as part of the overall resilience of the territory. The authors explained the first two steps in detail:

Achieving political awareness on the relevance of Digital resilience: There is a huge variation in the level of Digital resilience across LRAs; political will is a precondition for digital resilience to be achieved by a public authority, as LRAs are the most vulnerable and preferred target for hackers, and lastly, there are no standard methods for LRAs to quantify damage, assess the impact and evaluate the cost of digital non-resilience. For these risks, the authors recommend running awareness-raising campaigns addressed to LRAs; putting Digital resilience of LRAs high on the political agenda; facilitating the exchange of experiences between municipalities, especially in cooperation with motivated leaders; defining & suggesting ad-hoc methods for LRAs to assess cyber risks, vulnerabilities and potential impacts and cost of digital incidents, and debating the possibility of introducing the obligation on public authorities of non-payment of ransoms.

Defining the most feasible governance model for digital resilience: It is expected that EU legislation will be one of the main change drivers in the field. The study recommends to develop a non-disciplinary compliance monitoring system to understand the level of uptake of cyber-related legislative provisions across LRAs; creating an award/preferential mark for exemplary local authorities to help them access EU funds to consolidate their path; adopting innovative approaches to meet the increasing demand for ICT specialists within the public sector, using in-house arrangements or in liaison with the education and training sector and facilitating the identification of qualified ICT service providers at the territorial level.

Agnieszka Wawrzyk, *Head of Sector Secure Value Chain, DG Connect, European Commission*, then presented the recent proposal for an **EU Cyber Solidarity Act**. She started by introducing the **European Cyber Shield**, a tool to be used to strengthen common Union detection and situational awareness of cyber threats and incidents. This is to be complemented by a pan-European infrastructure of Security Operations Centers (SOCs) to build and enhance cyber threat detection, both at a national and cross-border international level. There will be financial support for its deployment, through a joint procurement of state-of-the-art tools and infrastructure, as well as grants. The European Cyber Shield will be based on the basis of information sharing, both at a Union level and within cross-border SOCs; on interoperability; and on security.

A second tool, the **Cyber Emergency Mechanism**, will be created to reinforce the preparedness of entities operating in critical and highly critical sectors and to strengthen solidarity by developing common response capacities against significant or large-scale cyber security incidents. It will provide

preparedness and mutual assistance actions, as well as an EU Cybersecurity reserve. The latter will be procured by 'trusted providers', based on strong selection criteria. If associated with the European Digital Europe Programme, third countries will be able to also benefit from these advantages.

A third tool, the **Cybersecurity Incident Review Mechanism**, will be developed to enhance Union Resilience and contribute to an effective response by reviewing and assessing significant or large-scale incidents. This will ex-post review and assess the risk of threats, vulnerabilities and mitigation actions. It can be requested by the CSIRTs network, the EU-CyCLONe or the European Commission.

III. Assessment of Digital Maturity of cities and regions

LORDIMAS is the name of a new online tool which will serve those in charge of digital transformation at regional, municipal and city levels to benchmark their digital maturity against their peers and to receive policy recommendations from more advanced players. CoR LORDIMAS Ambassador **Ufuk Kâhya (NL/Greens)**, presented this tool to the audience. He underlined its benefits of not only being able to compare their region/city to others but also knowing what next steps ought to be. LORDIMAS developer **Martin Gauk** from ESPON then showed the online page to the attendees to see how it ought to be used.
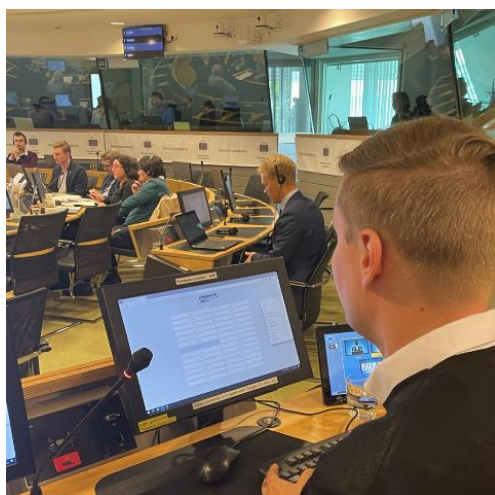
The beta version of LORDIMAS can now be seen at: LORDIMAS_beta v5.1 (espon.eu)
The official release of the tool is planned for October 2023. There will be a dedicated event with the LORDIMAS ambassador during the European Week of Regions and Cities.

Report of the Broadband Platform Meeting, held on 25 May 2023, Brussels

List of Participants

Broadband Platform Members and CoR Members

Ufuk KÂHYA *(ECON, SEDEC/Greens), LORDIMAS ambassador and CoR Member**,** Alderman of the municipality of 's-Hertogenbosch, The Netherlands*

Ilpo HELTIMOINEN *(ECON, NAT/ECR), Lappeenranta City Councilor, Finland*

Rait PIHELGAS *(Alternate/Renew), Member of a Local Assembly: Järva Rural Municipality Council, Estonia*

Declan MCDONNELL, *(CIVEX, SEDEC/EA), Member of a Local Executive: Galway City Council, Ireland*

Jacinth HORVATH *(NAT, SEDEC/PES), Member of Nagykanizsa Municipal Council, Hungary*

Michael MURPHY *(ECON, CIVEX/ EPP), Mayor of Clonmel Borough District, Ireland*

Florian SIEKMANN *(Alternate/Greens), Member of the Bavarian State Parliament, Germany*

Mindaugas SINKEVICIUS *(ECON, CIVEX/PES), Mayor of Jonava District Municipality, Lithuania*

European Commission

Franco Accordino, *Head of Unit, Investment in High-Capacity Networks, DG Connect, European Commission*

Silvia Adriana Ticau *and* **Hannele Lahti**, *Electronic Communications Policy, Implementation and Enforcement Unit, DG Connect, European Commission*

Agnieszka Wawrzyk, *Head of Sector Secure Value Chain, DG Connect, European Commission*

External speakers

Simona Cavallini, *Senior Researcher and* **Rossella Soldi**, *Managing Director, Progress Consulting*

Martin Gauk, *ESPON European Grouping on Territorial Cooperation*

European Committee of the Regions

Robert Ronstrom, *Deputy Head of Unit, Commission for Economic Policy*

Marek Bobis, *Policy Officer Digital Europe, Commission for Economic Policy*

Anke Schuster, *Policy Officer Digital Europe, Commission for Economic Policy*

Cristina Palacio Cano, *Trainee, Commission for Economic Policy*