High-capacity connectivity is vital in scaling Europe’s broadband networks across the continent, in the hope of guaranteeing Europe’s position at the forefront of the 4th industrial revolution.

Europe’s cable industry aims to pursue an objective of ubiquitous gigabit connectivity, ensuring that all are able to participate in the future potentials of fast, reliable and high-capacity network infrastructures.

From health to e-government, connected cars to the Internet of Things, the EU’s stance in the global digital marketplace is dependent on its ability to feed such sectors with the right tools to operate efficiently.

But there are challenges along the way. How does the EU maximise its connectivity potentials whilst also safeguarding consumer trust? How can networks be secured against attacks? How can competition law be made to foster innovation and development across the continent?

This special report looks into the many opportunities and challenges ahead for the EU if it is to deliver a connected future for all of its citizens.
Bridging the EU’s broadband divides: The importance of trust and security
Investment in ‘first class connectivity infrastructure’ a priority, Commission says
Delivering a connected future
The EU has long been plighted by patchy broadband coverage, so much so that previous Commission targets set out for 2020 were put to bed last year by the European Court of Auditors. But could 2019 prove to be a tipping point in the bloc’s connectivity potentials?

As part of its Europe 2020 strategy, in 2010 the EU set out a series of broadband targets, including the objective of providing by 2020 all Europeans with broadband connection of over 30Mbps.

However, towards the end of last year, the European Court of Auditors intervened in the pursuance of these objectives, citing the difficulties of rolling out fast broadband coverage across remote areas of the Union.

“Rural areas,” the report wrote, “where there is less incentive for the private sector to invest in broadband provision, remain less well connected than cities, and take-up of ultra-fast broadband is significantly behind target.”

That is not to say that EU member states don’t recognise the need for improvements to be made in the bloc’s broadband coverage.

France’s President Emmanuel Macron, for example, has made...
Continued from Page 5

ambitious pledges in this area, with the country’s Prime Minister Édouard Philippe announcing at the end of 2018 that the Treasury would invest €620 million in order to accelerate territorial coverage.

10G REVOLUTION

Against this backdrop, last week at the Consumer Electronics Show in Las Vegas (CES), three industry groups including Brussels-based Cable Europe presented their plan for bolstering broadband speeds from 1 gigabit per second to 10 gigabits per second worldwide. Known as the ‘10G’ plans, Cable Europe has described the measures as the “next great leap for broadband.”

Industry in the EU is starting to make moves in an area that has historically proved challenging. Last week, Cable Europe launched a white paper delivering policy recommendations, featuring a number of crucial areas for policymakers to take into consideration if Europe is to be as ambitious as previous targets have aimed at.

One such area is the importance of increasing trust and security of network infrastructures, a subject delicate for citizens across the EU.

Phil McKinney, CEO of CableLabs, a US research and development organisation centred about the cable operator industry, noted the importance of high-security standards when exchanging views on the matter with EURACTIV.

“To ensure the highest levels of security, there are best practices. Things like information sharing are vital when breaches do happen, in order to plug those holes to make it harder and less interesting for the bad actors.”

“If you raise your security bar, the bad actors will ignore you and go after somebody that is weaker. The challenge is, how do you raise the bar for everybody?”

Should security standards be led by the industry or by regulators? McKinney was clear in his stance. “Industry can move much faster than regulators,” he said. “Regulators need to think about unintended consequences, while the industry has been working away at increasing trust in the privacy and security of IoT devices in particular.”

IOT VULNERABILITIES

Meanwhile, with the ever-increasing demand for Internet-of-things (IoT) products, a new horizon of security threats are expected to hit servers.

The European Commission’s ‘Advancing the Internet of Things in Europe’ working paper, published in 2016 as part of the Digitising European Industry project observed that the main challenge for IoT devices remains “user trust” while “security and the protection of personal data issues are a key concern for a successful take-up of the IoT.”

In 2017, the EU’s cybersecurity agency ENISA also recognised the challenges ahead if the growth of connected devices is to reach projections of more than 30 billion connected devices worldwide by 2020.

EURACTIV spoke to ENISA’s IoT expert Apostolos Malatras on the security threats surrounding the use of connected devices.

“These types of products should come with security-by-design standards,” he said, adding that one of the major challenges for Europe is to ensure that the public is appropriately informed as to the risks surrounding specific sectors.

“With connected devices, some sectors haven’t taken into account that security measures are vital for the safe operation of the products,” he said. “The growing market for connected toys, for example, has a blind spot in taking into consideration the ramifications of not meeting proper security standards.”

Malatras’ warning in this respect is echoed by Ursula Pachl, deputy director general of the consumer group, BEUC, who recently raised a stark warning with regards to the security of connected toys.

She even told EURACTIV that some such devices should not even be kept in the home while security flaws still exist, highlighting the importance that manufacturers and network providers have in ensuring that connected devices are both safe to use as well as being cybersecure.

IOT UBIQUITY

The importance of security in IoT devices not only affects the consumer market. With connected device use on the up across a range of sectors, including health and transport, ubiquitous connectivity will be vital to ensure that public and private services can be carried out safely all across the continent.

High-capacity connectivity in cable networks can ensure the swift expansion of Europe’s broadband coverage and deliver such important services to people, but only if people are able to fully trust the products that they are operating.

Without the commitment to increase public trust through high-security standards alongside appropriate private investments in the field, many areas of Europe risk remaining alienated from the future high-speed revolution.
The cable industry’s ambitions of ubiquitous gigabit connectivity have long been hindered by a number of obstacles, including patchy coverage and consumer trust issues. Carlota Reyners Fontana explains what the EU Commission is doing to improve the bloc’s broadband gaps.

Carlota Reyners Fontana is the Head of Unit responsible for Investment in High-Capacity Networks, in the European Commission’s DG Connect.

She spoke to EURACTIV’s Samuel Stolton.

The European Court of Auditors have urged shelving EU targets of providing all Europeans with broadband connection of over 30Mbps by 2020 because of concerns over rural coverage.

The European Court of Auditors’ Special Report identified a number of challenges that EU countries still need to overcome in order to roll out the broadband infrastructures necessary to support the digital transformation of society and economy, as well as reduce the urban-rural digital divide.

The Commission continues to be aware of the importance of extending Europe’s broadband capacities. €6 billion of European Structural and Investment Funds were allocated to broadband for the 2014-2020 period. Additional support has come from the European Fund for Strategic Investments, the new Connecting Europe Broadband Fund, as well as the WIFI4EU initiative.

For the next budgetary period of 2021-2027, the Commission has proposed that EU support for very high speed connectivity continues, through instruments such as the European Regional Development Fund and the European Agricultural Fund for Rural Development, the digital part of the...
Continued from Page 7

renewed Connecting Europe Facility, and the InvestEU programme.

On the specific issue of the urban-rural divide, our Rural Action Plan focuses on the challenges of rural broadband, not least through the exchange of best practices through the Broadband Competence Offices network, targeted Member State missions, closer monitoring of broadband spending from the European Structural and Investment Funds, and updated guidelines on broadband investment.

A recent case study in the impact better broadband coverage can have in rural areas of Europe is in the UNESCO listed Danish island of Møn. As a winner of the European Broadband Awards, the area benefited from the installation of high capacity network installation. Can you talk a bit about how the area, not generally considered attractive for commercial broadband investments, benefited from the project?

The project provided a high capacity network to the inhabitants of a very small island (110 houses) located in the UNESCO world heritage area of the Wadden Sea, Denmark. It was driven by the efforts of local community volunteers who worked without support from the Danish broadband state aid scheme. They managed to get almost all houses on the island connected to a broadband network. This new connectivity infrastructure has also helped the island attract more tourists.

What obstacles are there in delivering fibre connections to these rural areas and how can these challenges be mitigated?

Bringing fibre infrastructure to households in rural areas is very expensive, and often there is not enough return for investment. The EU is financing such projects through structural funds and encourages private investment (with the recent reform of the regulatory framework that resulted in a new European Electronic Communications Code), to complement European and national funds.

A number of local initiatives finance the deployment of fibre by using local means, and our Broadband Awards have over the years recognised a number of such initiatives. The Cost Reduction Directive also includes a series of measures to reduce the costs associated with broadband deployment.

In terms of finding solutions to the EU’s broadband coverage challenge across rural areas, what type of relationship do you envisage in the future between fixed and mobile networks? Is convergence the way to go?

In the coming years, 5G is expected to be the enabler for all digital services by providing connectivity to people, wherever they are, in both urban and rural areas. Fixed-line and wireless services will increasingly become substitutes for each other from a user’s point of view. At the same time, the use of fibre infrastructures for 5G coverage can also make the extension of broadband coverage to local rural households that would not be connected otherwise more interesting.

The FTTH Council recently published research on the EU’s top countries in fibre broadband to the home. There is a significant disparity between those at the top of the list, and those towards the bottom. Why is this the case?

It is true that Fiber to the Premises (FTTP) – the main technology together with advanced cable networks supporting ultrafast broadband – is developing at a different pace in different EU countries. This can be for many different reasons, ranging from the geographical distribution of a country’s population to the quality of the existing legacy networks, availability of physical infrastructure, urban planning rules, market structure, market regulation choices, levels of broadband take-up and the availability in a country of online services that are reliant on higher speeds.

More broadly, a country’s socio-economic situation and the way in which it implements public support schemes can also be relevant. In general, FTTP remains still largely an urban technology led by commercial investment. However, in countries such as Portugal, Latvia and Denmark more than 50% of rural homes already have access to it.

In an age in which trust in digital structure is being tested, how important is it that broadband providers recognise the importance of cyber-security in their working methods? How is the Commission working alongside industry to ensure that trust in network infrastructure is taken seriously?

The Commission takes this issue very seriously and is continuing its work to increase cybersecurity in the EU. This is why we have always endeavoured to ensure that not only existing networks but also next generation networks will provide a high level of cybersecurity across the EU.

Under current EU rules, telecoms operators are already subject to clear obligations, defined by national authorities, to ensure the security of their networks. In addition, the EU now has a range of legal instruments, such as the NIS Directive, the EU Cybersecurity Act, and the new telecoms rules, to reinforce cooperation against cyber-attacks and enable the EU to act collectively in protecting its economy and society.

Continued on Page 9
In this vein, are self-regulatory measures, such as the certification framework as part of the recently adopted Cybersecurity Act, sufficient?

The recently adopted Cybersecurity Act creates an EU cybersecurity certification framework for ICT products and services. The cybersecurity certification framework is voluntary but it cannot be considered as a self-regulatory measure. It is about creating certificates.

Today in the EU a number of different cybersecurity certification schemes for ICT products exist. With the EU Cybersecurity Act we are creating a common framework for EU-wide valid cybersecurity certificate schemes: a comprehensive set of rules, technical requirements, standards and procedures to agree each scheme.

Each scheme will be based on agreement at EU level for the evaluation of the security properties of a specific ICT-based product or service. This certificate will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified cybersecurity requirements. ENISA, the EU Agency for Cybersecurity, will put in place and implement this certification process. The Commission, cybersecurity experts and national cybersecurity authorities have also an important role to play in this process.

The resulting certificate will be recognised in all EU countries, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

When we talk about bridging the Broadband divide in Europe and moving towards a culture of ubiquitous connectivity, how far-reaching could the future applications of broadband technology be?

In addition to what I mentioned earlier, 5G could also help to address the current broadband divide directly. For example, the possibility of terminating a fibre connection with 5G wireless fibre, allowing fixed wireless access at gigabit or quasi-gigabit speeds, could potentially offer a cost-efficient solution for very sparsely populated rural areas in particular.

5G will be one of the key building blocks of our digital economy and society in the next decade. The future infrastructure will help to create wide range of applications and benefit many sectors, from eHealth services to energy management and water quality control to Connected Automated Mobility.

From government initiatives and health projects that take advantage of high-speed and capacity networks, how realistic is it for citizens to envisage a future that is seamlessly connected? What needs to happen for this future to be realised?

Realising this vision involves investing in first class connectivity infrastructure as well as in education and skills, creating a business and regulatory environment where digital services can thrive.

Yet without stimulating and supporting network investments, the digital transformation is not possible. With this in mind, we have proposed that the digital strand of the Connecting Europe Facility post-2020 focuses on strategic infrastructure projects, such as gigabit connectivity to educational and medical centres and their surrounding areas, 5G connectivity along major transport paths, and very high quality connectivity for local communities. No European should be deprived of the benefits of such projects.

What's the most effective way for EU citizens to realise the benefits of future high-capacity and high-speed networks? Do you think there is a knowledge gap in this field, across certain parts of Europe?

Europe must seize the countless opportunities offered by the digital transformation. Investing in future-proof infrastructure is a key part of that, but we also need to ensure that citizens, wherever they live and whatever their background, have the skills they need to thrive in the digital future.

With this in mind, the Commission has set up the Digital Skills and Jobs Coalition, which brings together EU countries, companies, social partners, non-profit organisations and education providers who are committing to help people acquire digital skills.

The Coalition’s actions target citizens in general, the labour force, and ICT specialists, as well as modernising education, with the goal of providing all students and all teachers with the right tools and materials to upgrade their skills. The pilot Digital Opportunity traineeship programme also permits up to 6,000 students to acquire key knowledge and capabilities.
A connected Europe is closer than you might think. An explosion of new digital services is just around the corner, from autonomous driving to e-democracy and virtual reality.

Very high-speed broadband is at the heart of it. Cable’s gigabit networks will be central to delivering the benefits of digitisation.

What’s the role for policy makers? It’s creating and sustaining an environment which nurtures and nourishes investment in these networks. It’s a virtuous circle of investment, innovation, trust, scale and security which will deliver our joint goals.

The cable industry is poised to deliver on its 10G vision of a seamlessly connected future. Operators and policy makers share a common goal. We look forward to playing our essential part in making this a reality.

Further information:

The White Paper on Delivering a Connected Future can be downloaded on https://eurac.tv/9QLC. Learn more about 10G here: www.10gplatform.com
For information on EURACTIV Manifesto Reports...

Contact us

Davide Patteri
Public Affairs Senior Manager
davide.patteri@euractiv.com
tel. +32 (0)2 788 36 74

Samuel Stolton
Digital Affairs Editor
samuel.stolton@euractiv.com
tel. +32 (0)2 226 58 26