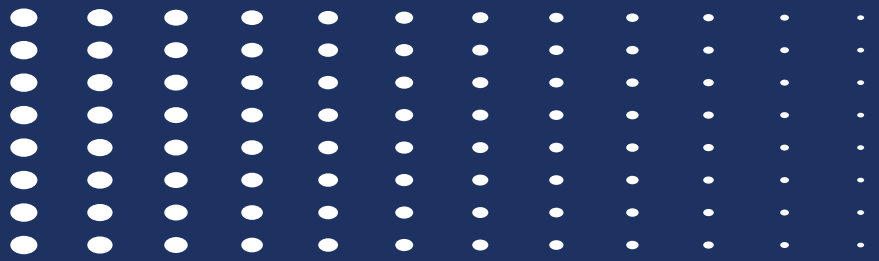
Choose a Smarter Future

A CONTRIBUTION TO EUROPE'S NEXT DIGITAL POLICY


Choose a

Smarter Future

A CONTRIBUTION TO EUROPE'S NEXT DIGITAL POLICY



Foreword

CHEN LIFANG
Corporate Senior Vice President
Director of the Board
Huawei Technologies Co., Ltd.

FOREWORD

With the rapid development of 5G, AI and the Internet of Things, the door to a smart society is open. The underlying networks, in particular optical fibre and 5G, are the intelligent equivalent of road infrastructure. Artificial intelligence is the equivalent of cars running on the highway, reaching all dimensions of people's lives. Figuratively speaking, digital talent can be represented by the drivers.

Smart society requires wider and better roads (fundamental networks), better cars (AI applications), and more and better drivers (digital talent). Therefore, policy-makers should review regulations, incentivise digitalisation of all industries, facilitate roll-out of high speed networks, and cultivate more talent.

OUR CONTRIBUTION TO THE EUROPEAN ECONOMY

Huawei employs more than 12,000 people in Europe, including about 2,400 R&D staff in 18 centres.
Our contribution to the European economy is equally significant in terms of taxes and supply. Between 2009 and 2018, Huawei procured a total worth of about EUR 33 billion in Europe. This figure is expected to reach EUR 35 billion between 2019 and 2020.

Europe is getting ready for the next five years, with an elected European Parliament, an incoming European Commission, and a forthcoming decision on the next Multi-Annual Financial Framework (2021-2027). EU strategic goals are already being reviewed and redefined, with digital policies high on the agenda across all areas.

As a global provider of end-to-end digital solutions with a significant presence in Europe, Huawei has a unique perspective that we would like to share with the newly elected representatives in the European institutions.

With regard to digital policies, the last EU legislative period focused on the Digital Single Market (DSM), a comprehensive legislative programme. The DSM initiative as well as the previous Digital Agenda were embedded in the overall Europe 2020 strategy. The EU will soon have to decide on a new architecture for its socio-economic strategy. On 20 and 21 June 2019, the European Council outlined a Strategic Agenda in which digital policy plays an important role, confirming its ever-increasing importance.

A company like ours can bring most value by raising technology issues and highlighting market and policy trends which we have seen emerge at a global level. As a technology innovator, we consider digital as a crucial enabler for achieving all UN Sustainable Development Goals. As part of the global digital industry, we are guided by the conviction that our economies should be open to each other, in particular as we share challenges from climate and poverty to productivity slowdown. We are encouraged by the G20 Leaders' Declaration that says right at the beginning: *"We will work together to foster global economic growth, while harnessing the power of technological innovation, in particular digitalization, and its application for the benefit of all."*

Against this background, we have singled out ten challenges for digital policy-making over the coming five to ten years which require particular attention. We hope that this contribution to the forthcoming digital transformation strategy of the EU will bring novel insights and stimulate some thoughts about what will matter most and why.

Introduction

INTRODUCTION

The impact of digitalisation is being felt across the economy and society at a greater scale than ever before. Digital policy discussions are no longer confined to technology experts, telecommunication regulators and economic ministers. Strategic orientations about digital issues are increasingly set by heads of state and government. On the surface, this evolution is driven by a couple of technology developments impacting people's lives.

Smartphones and their plethora of apps have changed lifestyles and created new business models through features such as mobile payments, navigation and mobile identity management, to name just a few. The number of **connected** people (today about 4 billion) and devices (today about 30 billion) is on the rise, turning connectivity into a forceful expression of global ambition, far surpassing mere economic stakes. The impact of **social media** on politics and social cohesion (e.g. influence on elections, radicalisation and hate speech) has raised the political stakes significantly. **Artificial Intelligence** (AI) is impacting the entire economy and is triggering both excitement about its potential and concerns about ethics and the future of labour.

Yet we need to go deeper than describing observable trends to work out which challenges the digital economy is facing, what is holding back progress for people, and which potential policy responses could make a difference. To identify these challenges, we have been guided by three considerations, which are interlinked and not strictly separable.

First, **progress for all people in all countries**. Digital transformation is on the agenda of almost all international organisations, such as the UN, World Bank, IMF, OECD and WEF. The underlying rationale of this paper is not to give recommendations on how to lead; it is not about the competitiveness of one region or country over others, but about welfare and prosperity for all and about dealing with climate change and protecting the world we all live in. In this context, we highlight productivity growth and the green digital economy as the first two digital challenges, followed by skills development.

Second, **infrastructure**. Fixed and mobile broadband connectivity is the foundation of digital transformation. Much less visible than the smart devices that have invaded our everyday lives, it is easy to forget that without the heavy infrastructure required to provide them with connectivity, smartphones and computers would be hardly more than toys and typewriters. The network turns them into productivity tools. We also think that Europe should reflect on the role of its telecom operators who need to invest in and build essential parts of the infrastructure. Smart cities and connected mobility are key investment priorities for building Europe's future digital ecosystem.

Third, **innovation**. Leaving aside their intrinsic value and considering science and technology from an economic and social perspective, they generate value in the form of productivity growth and social progress when they are transformed into innovation. Behind every digital agenda is an innovation agenda which does not focus on technology as such, but on the obstacles to overcome and the societal climate to encourage entrepreneurship. When looking at emerging technologies and considering their potential economic and social impact over the coming years, AI is the one that stands out.

Finally, there is cyber security which cuts across all digital issues and is a challenge wherever computers and networks are involved. In this paper, we have taken a holistic and policy view, as these aspects will determine our collective success in the cyber field to a far greater extent than the vast array of detailed technical requirements for the digital ecosystem.

TEN **DIGITAL** CHALLENGES FOR **A SMART FUTURE**

10

TEN DIGITAL CHALLENGES FOR A SMART FUTURE

1. **Macro-economic reforms and digitalisation: time for a marriage**
2. **Green digital and green by digital: we need to aim at both**
3. **Digital skills: do we all need to learn how to code?**
4. **Gigabit society: what about the rural areas?**
5. **5G: it is about more than downloading a video in three seconds**
6. **Telecom operators: Europe's underestimated assets**
7. **Smart cities: why does it take so long?**
8. **Connected mobility: are we ready for a big move?**
9. **Artificial Intelligence: is it really a global race?**
10. **The never-ending story of cyber security: who writes the script?**

Executive Summary

Digital policies are playing an increasingly important role in the EU's overall socio-economic strategy. As Europe is deciding on a new policy architecture for the next five years, it must ensure that technological innovation delivers inclusive and sustainable progress.

OVERCOMING THESE TEN CHALLENGES FOR DIGITAL POLICY-MAKING WILL PLAY A KEY ROLE IN ACHIEVING THIS OBJECTIVE:

1. **Digital policy should become an integral part of a macro-economic policy agenda.** The European Semester, as the framework of choice for implementing this, should systematically include a country-specific recommendation to enhance the use of digital technologies in the Member States.
2. **The digital industry must step up to become greener.** The great potential of 'green by digital' must be accompanied by policies to counter the 'rebound' effect offsetting initial benefits.
3. **Digital skills should be one of the hard skills everyone must acquire.** This is a crucial task for education policy. Companies also must invest more in training and in upgrading the digital skills of their employees.
4. **The EU should set the most ambitious target for full gigabit coverage across its territory.** A hybrid infrastructure consisting of fibre networks and 5G enabled 'Fixed Wireless Access' will be the key to achieving it.
5. **5G will deliver a quantum leap for people and the economy if policy-makers help address deployment issues.** These include spectrum, local regulations, security requirements, and electromagnetic exposure concerns.
6. **Europe needs to recognise the role of its telecom operators in building gigabit connectivity and as global players.** This involves helping them become more profitable by reducing the regulatory burden and by opening up more investment opportunities.
7. **Smart cities, at the centre of digital transformation, need more support to reach their full potential.** Policy-makers need to address issues related to mindset (overcoming silo thinking), money (investments are hampered by a lack of business cases) and management (complexities create a dissuasive level of risk).
8. **The EU should approach 'connected mobility' by looking at the bigger picture.** A 'Master Plan' could set out an implementation agenda guiding the actions of the many actors that are involved.
9. **Artificial Intelligence will be of great benefit to humanity and should be addressed as such.** It is not a race. It is about innovating, finding practical solutions to ethical issues, and working together at global scale.
10. **As a shared responsibility, cyber security remains on any digital agenda.** Collectively we should strive to find more systemic solutions, making cyber-attacks much more difficult right at system level. More international cooperation, including global companies, to fight cybercrime will make the digital economy a safer place.

1. MACRO-ECONOMIC REFORMS AND DIGITALISATION: TIME FOR A MARRIAGE

PRODUCTIVITY MATTERS

Productivity growth drives prosperity and is a prerequisite for social inclusion. Labour productivity tells us how much an economy gets out of one hour of work on average. Total factor productivity shows how efficient an economy employs its labour and capital. In advanced economies, it manifests itself in higher average income per capita with more leisure time.

Productivity growth is determined by many factors such as education, good governance and efficient institutions, but the most important long-term driver is progress in science, technology and innovation. We refer to today's technology powerhouse as 'digital transformation'. When we speak about the 4th industrial revolution, we mean a digitally empowered surge of productivity growth.

There is an issue however: productivity growth is not a deterministic function of more digital investment. For the investments to bear fruit, we need the economy to transform, the society to adapt, habits to change, education to be reformed, and many more complementary assets to evolve in parallel.

WHAT'S AT STAKE? A LOOK INTO THE RECENT PAST

In July 1987, the economist Robert Solow, Nobel Prize winner, observed that the presence and impact of computers seemed to be 'everywhere except in the productivity statistics'.[1] This phenomenon is called the **'Solow Paradox'**.

It can be understood as a gestation period during which digital capital and complementary assets are being accumulated so as to fully exploit the underlying technology.

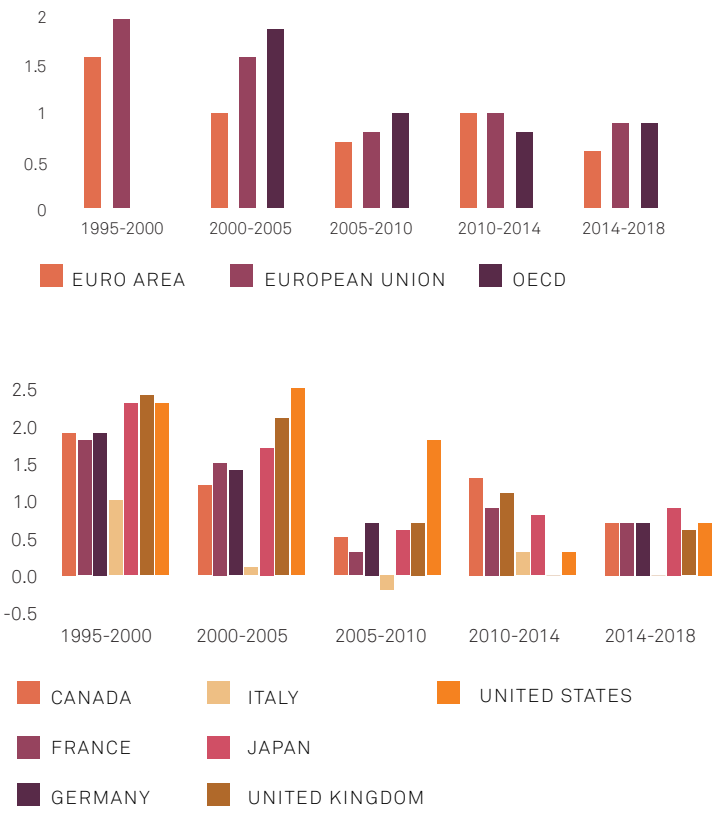
Investment levels preceded productivity boosts, which eventually appeared in the national accounts' data in many countries from 1995, resolving the Solow Paradox – but only temporarily.

Productivity growth has been slowing down again since the mid-2000s. The OECD asserts: ***"The productivity slowdown has multiple and partly interlinked causes, ... The aggregate productivity gains from digitalisation have not been sufficiently large to offset these headwinds, at least not to date."***[2]

McKinsey takes a similar stance: ***"The most challenging finding is that diffusion of best practices is not pulling the rest of industry along. The natural force of competition among firms should work to prevent the dispersion of productivity from widening continuously and something appears to be blocking that process."***[4]

This is in line with research carried out by the London School of Economics (LSE) in cooperation with Huawei, which concludes that the most likely explanation of the current slump in productivity growth lies in the notion of another implementation lag. Our current era is plausibly a time when firms are still working out strategies for utilising the full potential of AI and robotics, as well as other complementary general purpose technologies such as the cloud, big data analytics and 5G. The LSE's research predicts a productivity resurgence powered by digital technologies in 10-15 years' time.[5]

OECD COMPENDIUM OF PRODUCTIVITY INDICATORS 2019[3]



THE EUROPEAN SEMESTER:
AN EXCELLENT FRAMEWORK

An appropriate framework for including a macro-economic approach in the future digital policy is the European Semester. One of its key outcomes are so-called Country-Specific Recommendations (CSRs) which have a politically binding character and are in certain cases elevated to legal obligations.

Until recently, digital elements have not been a major subject of CSRs, which focused on public deficits, pension systems, cost competitiveness, overheating housing markets, labour market reforms and education performance. This has changed with this year's European Semester:

"Digitalisation is a key lever of productivity, competitiveness and growth. Traditional sectors and small and medium-sized enterprises are particularly lagging behind in their digital transformation. The EU as a whole must speed up the process. Adequate support is necessary. This mandates a better alignment of Union, Member States and regional policies, and pooling of public and private resources to increase investment and develop stronger synergies in the digital economy and society."[6]

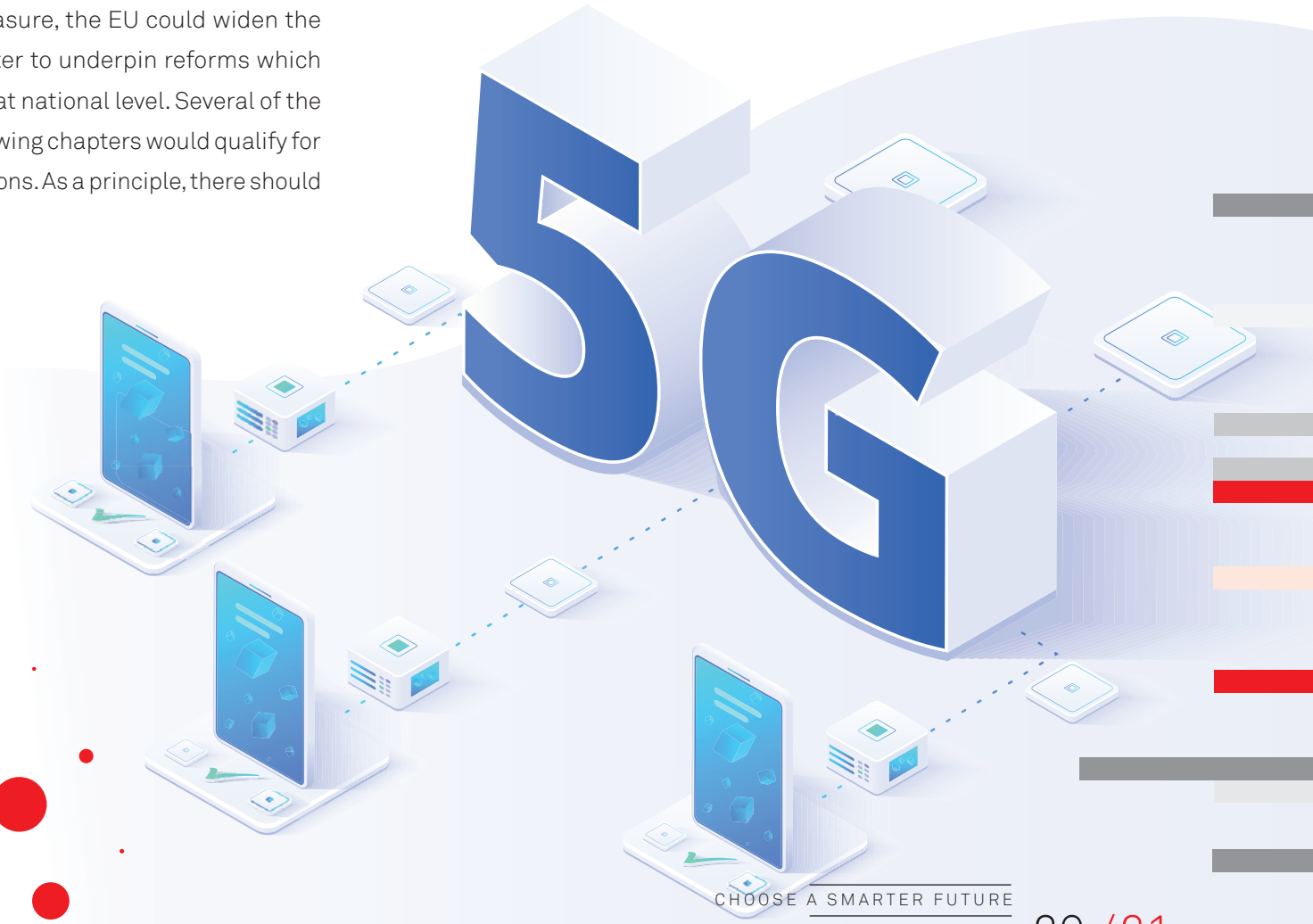
Consequently, in the 2018/19 European Semester, there are 19 CSRs directly addressing digital issues, ranging from broadband, public e-services, digital skills and digitalisation of SMEs, to making digital an investment priority. This is an important first step, as digital has been recognised as part of the reform agenda of the EU. Going forward, the underlying country analysis could follow a more systematic and consistent method, covering digital issues as a prerequisite for productivity growth and societal transformation in CSRs.

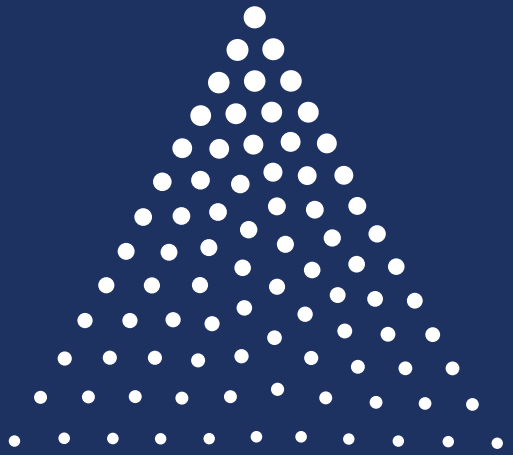
Such a systematic approach could address factors that hamper the growth and take-up of digital technologies across the economy, including

- digitalisation gaps at company level
- investment needs in fields such as smart cities and connected mobility
- reforms of educational systems to make use of digital opportunities
- reforms of public services to efficiently use digital services, and
- overcoming obstacles to deploying 5G networks.

OUTLOOK

Digital policy must become a part of macro-economic policies. Otherwise, complementary investments – which help to unleash the productivity potential of digital technologies – will remain suboptimal. As a practical measure, the EU could widen the scope of the European Semester to underpin reforms which support digital transformation at national level. Several of the challenges analysed in the following chapters would qualify for country-specific recommendations. As a principle, there should be one digital CSR per country.





2. GREEN DIGITAL AND GREEN BY DIGITAL: WE NEED TO AIM AT BOTH

DIGITAL GREEN

We need to be realistic and optimistic. We need to acknowledge that the digital industry, i.e. data centres, computers, smartphones, networks and IoT devices, contributes to global greenhouse gas emissions. How much is a question that is not easy to answer.

According to a 2015 report[7] by the Brussels-based Global e-Sustainability Initiative (GeSI), information and communication technologies (ICT) were responsible for about 2% of global greenhouse emissions, i.e. the level of the aviation sector in 2017. A 2019 study[8] by the Paris-based think tank 'The Shift Project' puts this share at a higher level and, more importantly, with a rising trend: 3.7% in 2018, up from 2.5% in 2013.

This is one of the most important challenges ahead of us: digital must become greener. At the same time, we need to make better use of digital technologies for reducing energy, emissions and waste.

The world will become more connected which will trigger a trend towards more consumption of electricity and raw materials for digital purposes. The industry needs to respond and become more energy and resource-efficient, and this must become a permanent and verifiable endeavour. With increased importance in the world economy comes increased responsibility. **We cannot promote digitalisation without promoting the reduction of the carbon footprint of the digital industry.**

Fortunately, this is already happening. Leading ICT companies follow environmental standards, such as ISO 14040 and 14044. They adopt circular economy practices and pay attention to resource efficiency, durability and recyclability.

SOME POSITIVE DEVELOPMENTS

- **Data centres** are increasingly being built in geographies that reduce the need for cooling (air conditioning) drastically. The industry is deploying more energy-efficient processors. Electricity for big data centres is typically generated by hydrogen and solar power.
- Huawei is working on **AI solutions** to shut down energy-consuming parts of telecom networks when they are not needed without problems for connectivity.
- **5G** consumes only 10% of the electricity per bit compared to 4G thanks to features including better heat dissipation, chip design and algorithms.
- **Devices** are built using harmless materials and more recycled materials.

The industry needs to do more in all fields and benchmark progress. Sustainability reports should contain detailed information about accomplishments and convey a transparent account of these efforts.

GREEN BY DIGITAL

Greenhouse emissions originate mainly from five activities: energy supply, transport, buildings, agriculture and industry, more or less in this order of magnitude. This is where the focus of Green by Digital should be placed.

Digital technologies contribute mainly through reducing transaction costs, real-time usage of data, discovery of interdependencies, and rationalisation of processes.

Many studies refer to digital technologies as a potential contributor to reducing the global carbon footprint. The previously mentioned study by GeSI explores this potential and **concludes that digital could save ten times the CO_2 it generates itself.**

A 2018 report[9] for the Commission also underlines the importance of digitalisation in reaching the climate objectives, stressing however the 'rebound' effect which runs counter to the initial positive effects. For instance, a better traffic flow can incentivise people to use their cars more, or a better parking system can incite people to use their car to enter the city instead of public transport. These 'rebound' effects are substantial and must be taken into account.

The report states: ***"Digitalisation will be a key enabling factor, both to allow action at system level, to increase efficiency, to deploy a (semi-)circular, dematerialised, service-oriented and shared economy, and to ensure that citizens become engaged in this transition."***

A more recent publication[10] by a number of computer scientists analyses the potential of artificial intelligence (AI) in ten areas, ranging from transport to manufacturing and agriculture. They focus on the mechanism through which machine learning could provide insights to reduce CO_2 emissions, and also assess potential rebound effects.

APPLICATION AREAS FOR GREEN BY DIGITAL:

- **Electricity Supply:** AI real-time predictions on how much electricity is needed can reduce reliance on polluting stand-by plants. This allows for better balancing of demand and supply in the light of a growing number of variable energy sources (solar, wind). Smart meters generate transparency for users and allow for better consumption control. Data collection helps improve the planning of electricity supply and the assessment of how many plants need to be built.
- **Transport:** Digital solutions could include scheduling and routing of freight operations to reduce the number of trips, smart parking systems avoiding unnecessary search drives, or smart pricing to enter cities.
- **Buildings:** The energy consumption of buildings could be reduced (by around 15%) by taking multiple factors such as weather forecasts and building occupancy into account. Air-conditioning management systems are amongst the most promising measures.

For many of the examples above, certain solutions already exist, such as traffic information systems, automatic light switch off, and data analytics. However, we still need to see mass deployment. Why is the market not deploying these solutions at large scale when there is so much potential to lower energy and other costs?

There seems to be a typical externality problem involved whereby private investors cannot capture all the benefits. In many cases a 'chicken-and-egg' problem also holds back private investments: You first need an infrastructure in place which connects IoT devices in order to justify the investment in services.

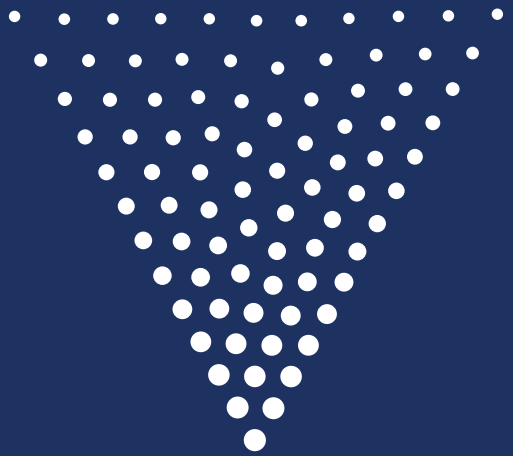
How to unleash the potential of digital technologies to tackle climate change deserves a substantial policy response on two fronts. First, public investments will be needed (for instance supporting smart cities) or at least better coordinated and more focused. Second, policy makers can help the private sector to agree on standards, overcome market fragmentation, develop missing skills, and raise awareness.

OUTLOOK

The potential of digital technologies to contribute to tackling climate change is substantial, but as of today remains underexploited. This brings us back to the point made in the first chapter: complementary investments, skills and processes are required to reap the benefits of technology.

Digital policy should look beyond the boundaries of individual technologies and break down the barriers to their deployment. Standards are one tool. Data is another. Where the collection of private data clashes with privacy provisions, implementation rules and more precise guidance from regulators could help. Last but not least, the rebound effect needs to be tackled, for instance through solutions such as traffic-appropriate road pricing models and making public transport more attractive.

3. DIGITAL SKILLS: DO WE ALL NEED TO LEARN HOW TO CODE?



To some extent, yes. Whilst not everyone needs to learn how to code, a certain understanding of how computers work is becoming a 'must know' for all citizens, and increasingly for employability or running a business or public service. According to the Commission's latest Digital Scoreboard[11], only 6% of EU citizens have ever written a computer programme (interestingly, this figure is almost 14% in Denmark). What we need to define is what exactly a 'certain understanding' involves.

When launching its first 'Code Week'[12] initiative in 2014, the Commission set out its rationale as follows:

"Learning to code helps us to make sense of the rapidly changing world around us, expand our understanding of how technology works, and develop skills and capabilities in order to explore new ideas and innovate."

Computers, or micro-processors, are everywhere, and need software to do something useful. Understanding programming is an essential part of digital skills, which, however, encompass many more elements than writing computer code. The question policy-makers should ask themselves is who needs which digital skills: different people and organisations have different needs, and they need to be addressed at different levels of education. In other words, policy concepts must differ depending on the context in which these skills are needed.

It is a challenge for policy-makers to categorise different levels of skill sophistication and to make them concrete and measurable. One interesting concept is the 'Digital Competence Framework'[13] developed by the Commission which is gradually being adopted by many organisations. This could be applied much more systematically across the different policy areas.

As mentioned in the context of macro-economic reforms as part of the European Semester (see chapter 1), digital skills have received prominent attention as part of a move to upgrade skills. These recommendations need to be implemented by Member States.

We suggest distinguishing three aspects which relate to different areas of policy-making, each covering different levels of sophistication, from basic to expert level:

1. DIGITAL COMPETENCES FOR CITIZENS

Just over 30% of EU citizens have digital skills above the very basic level. 40% of people active on the labour market do not possess even basic skills. A certain level of digital expertise is advisable for everyone, including the elder generation, for at least two reasons:

- **Our increasing dependence on digital services and access to the internet:** digital technologies are mainstreamed into all aspects of our daily lives, and the number of services that are

offered exclusively online increases every day. A lack of basic digital literacy is becoming a handicap in this context.

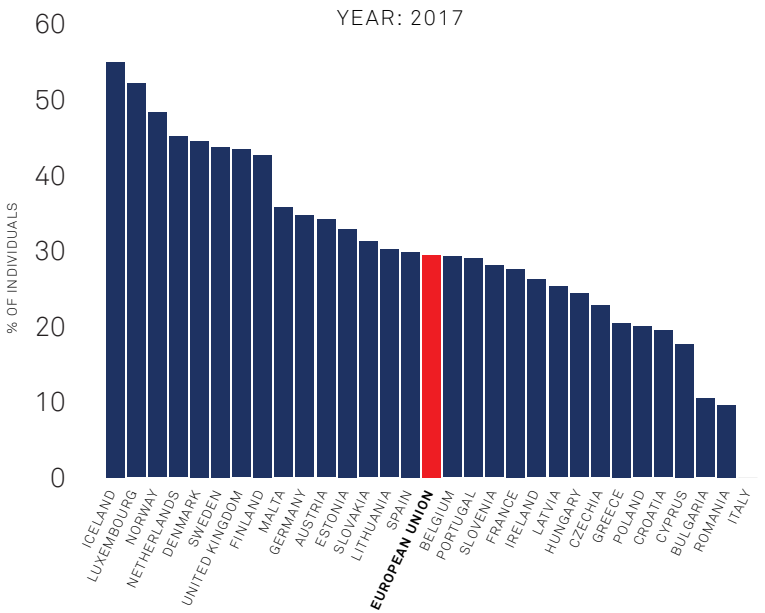
- **Cyber security:** using digital services requires a basic understanding of how to mitigate risks. These also include online manipulation: social media are becoming the mass media of the future, in particular for the younger generations. A basic understanding of the concept of botnets, AI algorithms, private data exposure and fake news (in particular fake videos – see chapter 9) is becoming a vital part of general knowledge.

The need for generalising digital expertise triggers the question of which digital skills should be taught at schools, and at what level. Views differ amongst and even within countries on how to translate the digital age into curricula and teachers' training. Some believe digital skills are for professionals, and schools should focus on general knowledge, critical and logical thinking, the ability to communicate and creativity. Others see coding and related digital skills as elementary modern skills which children need to acquire like reading and writing. Currently, about 30% of EU citizens have received some ICT skill training at school.

The competence for these issues lies at the national level, with the EU playing a stimulating role, financing pilot projects, promoting mutual learning and carrying out benchmarking. As set out above, the European Semester considers education a key structural factor for economic progress: ten Member States received recommendations on digital skills development. The EU could step up its efforts and in particular improve the evidence base and promote good practices amongst the Member States.

DIGITAL SKILLS INDICATOR (ALL INDIVIDUALS), LEVEL: ABOVE BASIC

YEAR: 2017



EUROPEAN COMMISSION, DIGITAL SCOREBOARD

2. DIGITAL SKILLS FOR EMPLOYABILITY

Digital skills are part of the broader issue of the future of work. In addition to 'hard' computer-related skills and knowledge, digitalisation will require 'soft' skills, such as creativity, conceptual thinking and team work.

Respondents to a representative 2017 EU poll[14] were concerned about the impact of digital technologies on the job market:

- About 20% of EU workers considered their ICT skills as insufficient
- 74% of respondents expect that due to the use of robots and artificial intelligence, more jobs will disappear than new jobs will be created
- 72% of respondents believe robots steal people's jobs
- 44% of respondents who are currently working think their current job could at least partly be done by a robot or artificial intelligence.

These results are confirmed by other surveys. For instance, a 2017 US poll[15] found that 72% of adults said they were worried about a future where robots and computers can perform human jobs.

The impact of digital technologies on employment has become a widely discussed topic. Will digital technologies, in particular robots and artificial intelligence, destroy more jobs than they create? This is one of the questions being asked over and over again. The answers oscillate between a doomsday scenario of mass unemployment and an optimistic outlook towards a better future for all thanks to digital transformation.[16]

One of the most recent analyses available at the time of drafting this paper is the *Future of Jobs Report 2018*[17] published by the World Economic Forum. It concludes:

"Nearly 50% of companies covered by the report 'expect that automation will lead to some reduction in their full-time workforce by 2022, based on the job profiles of their employee base today. However, 38% of businesses surveyed expect to extend their workforce to new productivity-enhancing roles, and more than a quarter expect automation to lead to the creation of new roles in their enterprise.'"

The study expects a ***"significant shift on the frontier between humans and machines when it comes to existing work tasks between 2018 and 2022. In 2018, an average of 71% of total task hours across the 12 industries covered in the report are performed by humans, compared to 29% by machines. By 2022 this average is expected to have shifted to 58% task hours performed by humans and 42% by machines."***

Consequently, by 2022, more than 50% of all employees will require significant re- and up-skilling.

3. DIGITAL TALENT

In the past, particular attention has been given to the perceived lack of ICT professionals[18]. There have been several studies to highlight this skills gap of ICT professionals. A 2018 study for the Commission[19] for instance estimated that there will be about 500,000 unfilled jobs for ICT professionals in the EU by 2020. An earlier forecast made in 2013 put this figure at 900,000 (which gave rise to the set-up of the jobs coalition). This variation in estimates has prompted critics to argue that the numbers could be overstated[20].

The statistical office of the Commission (Eurostat) has also published a survey[21] indicating that about 5% of EU enterprises report difficulties in finding ICT professionals on the labour market. This is not necessarily a contradiction, as only 20% of companies employ ICT specialists. However, it indicates that the results should be interpreted carefully. Similarly, according to Eurostat, the number of ICT professionals employed across the EU is about 8 million (2017), which means around 6% of vacancies remain unfilled from a static point of view. Yet, the job market is dynamic and therefore policy-makers should provide more data on actual vacancy fluctuations over time to paint a realistic picture.

In the medium and long term, demand for digital talents will increase. Europe would be well advised to grow interest in science and mathematics amongst the younger generation. Whilst the skills needed for the digital age are broader than these subjects, digital transformation will require digital talents in big numbers.

OUTLOOK

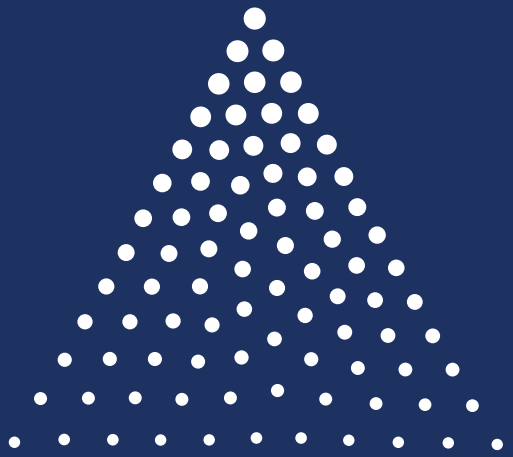
How best to respond to the challenges of the digital age with respect to education, life-long learning and acquiring skills is one of the most complex ones amongst the ten digital issues.

It is often argued that people need more soft and leadership skills rather than digital skills. However, this is not an 'either or' situation. Digital skills now belong to the category of hard skills such as reading, writing and maths. Education systems must adapt to ensure young people have an adequate level of digital competency.

Companies could be incentivised to provide training, not only as a reaction to short-term needs but with a digital strategy in mind. Future jobs will involve working alongside AI systems and physical robots, and the workforce needs to be prepared for this new scenario. To this end, the potential of e-learning services could be exploited to a much larger degree.

The EU could consider a more joined-up approach combining existing instruments and programmes with the European Semester recommendations providing guidance.


4



4. GIGABIT SOCIETY: WHAT ABOUT THE RURAL AREAS?

INFRASTRUCTURE UPGRADES:
DEFINING OUR AMBITION

Since the early 2000s, broadband connectivity has been on the European policy agenda. The current Digital Agenda targets 30 Mb/s coverage for all households and 100 Mb/s subscriptions for 50% of households by 2020. As things stand, the EU will almost but not completely reach the first objective (2018: 82%), whilst the second objective will be more difficult to attain (2018: 30%), in particular regarding actual subscriber rates.

In 2016, the Commission further raised the bar: according to its 'Gigabit Strategy', all households should have access to 100 Mbps, upgradable to 1 Gb/s (which indicates a preference for fibre-based connections) and all schools, transport hubs and main providers of public services as well as digitally intensive enterprises should gain symmetric 1 Gb/s access by 2025.[22] These more challenging goals could widen the digital gap between urban and rural areas.

We can broadly distinguish two kinds of upgrading challenges:

- In urban and partly in sub-urban areas, copper or coax-cable connections typically offer up to 100 Mb/s and even more. The incentives to pay a premium to upgrade to fibre and Gb/s speed are therefore limited. In addition, deployment can be expensive without access to an existing passive infrastructure (e.g. ducts).
- In rural areas, long distances, low population density and geographic characteristics (forests, hills and lakes) make deployment of fast networks expensive, and revenues are too low to justify significant investments.

THE CONNECTIVITY CHALLENGE:
SHARING THE COST

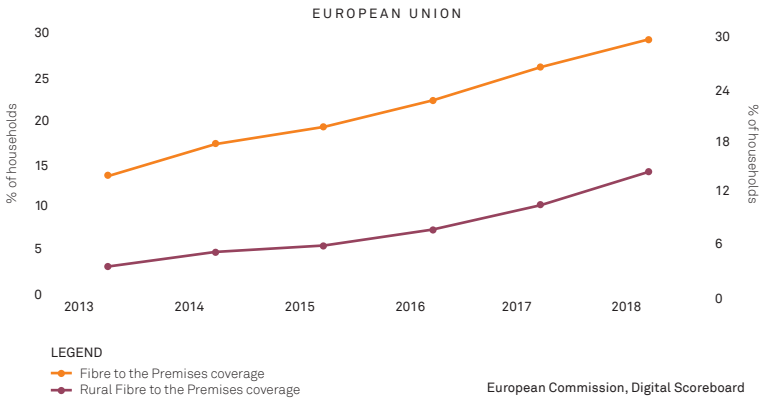
The political aspirations are in contrast with the market reality faced by private operators who need to see a return on their investments while facing stiff competition and strong regulatory requirements. Incumbent operators, who bear most of the regulatory burden, have long pleaded for less regulation whilst new entrants have taken the opposite view as far as access regulation is concerned.

To tackle these economic disincentives to invest in broadband, the EU has been implementing a number of policies and funding programmes, amongst them the 'Broadband Cost Reduction' Directive, a 'Broadband Investment Guide', the 'Connecting Europe Facility' and the usage of 'Structural Funds'. Individual Member States have also taken measures and implemented subsidy schemes (partly co-financed by the above-mentioned EU Funds).

The new electronic communications code ('The Code') adopted by the EU in December 2018 explicitly sets a connectivity objective. It includes a 'co-investment' scheme aiming to achieve a better division of the financial burden from regulation. As the final provisions are fairly complex, however, national regulators will struggle to put this into practice. Considering the strategic importance of the connectivity objective, European legislators might want to consider an early review of this particular clause in the light of recent experiences.

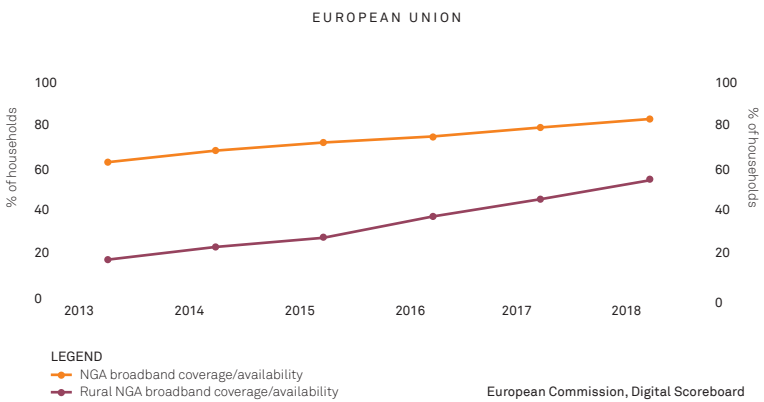
THE DIGITAL SCOREBOARD OF THE COMMISSION SUMMARISES THE STATE OF PLAY AS FOLLOWS:

Rural Fibre to the Premises coverage/availability (as a % of households), by Total and Fibre to the Premises coverage/availability (as a % of households), by Total



European Commission, Digital Scoreboard

NGA broadband coverage/availability (as a % of households), by Total and Rural NGA broadband coverage/availability (as a % of households), by Total



European Commission, Digital Scoreboard

Going forward, European policy-makers will have to make a strategic choice between a 'business as usual' approach and an ambitious agenda with a set of gigabit targets. The latter will only be meaningful if significant implementation efforts are made. **A gigabit strategy only makes sense if coupled with a rigorous execution agenda**. The 2018 report of the Court of Auditors on Broadband in the EU Member States confirms this.[23]

The EU and its Member States would need to provide adequate funding to overcome market gaps. A review of state aid implementation would also be required, not to relax competition, but to make it more practical. For instance, instead of deciding project by project whether an area is non-competitive, authorities could determine on the basis of objective criteria which areas can be generally financially supported.

If a gigabit society is the vision, how much geographic coverage should we aim for? Is a 100% target realistic? How do we connect rural areas?

With appropriate network architecture, 5G coverage on the basis of 700 MHz is a viable option, even for truly remote and geographically challenging areas. However, these solutions will not offer speeds close to the gigabit target. A practical solution for gigabit connectivity lies with 'Fixed Wireless Access' delivered by 5G on the 3.6 GHz and 26 GHz bands. Linked to the backbone with fibre or micro-wave, this will provide up to 10 Gbit/s download speeds, giving individual households a fibre-like experience. **Thus, future gigabit connectivity should be a hybrid of fibre and 5G-empowered fixed wireless access (FWA) to the premises.**

OUTLOOK

Policy-makers need to decide on the level of ambition of future connectivity targets and to ensure an adequate execution agenda. We encourage the EU to set the most ambitious target for full gigabit coverage.

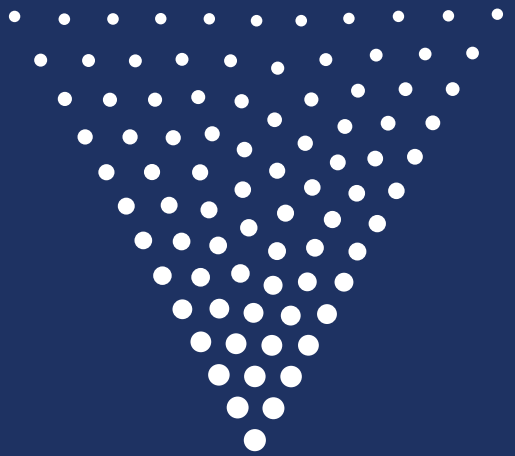
The corresponding infrastructure, based on fibre and 5G connectivity, would be an essential building block for digital transformation, triggering productivity growth and generating significant social benefits (positive externalities) for businesses, employees, students, consumers and citizens.

EU connectivity targets could become more binding for Member States – for instance as part of country-specific recommendations – and not be altered by national broadband strategies leading to a patchwork of efforts. For this to happen, we believe that policy-makers at the highest level, i.e. the European Council, will have to make this commitment.

An ambitious agenda would also send an important signal to global investors that Europe will invest and innovate its way to a smart future.

4

5. 5G: IT IS ABOUT MORE THAN DOWNLOADING A VIDEO IN THREE SECONDS



A NEW PARADIGM

Yes, 5G will allow incredibly fast downloads of 4k or 8k movies. Consumers will enjoy a superior video experience compared to 4G. However, 5G is about much more: it will offer a versatile communications platform, not just for consumers, but, importantly, also for vertical industries and applications, triggering a holistic transformation process through the new opportunities this entails. What EU policy beyond the current strategy is needed to make this transformation a success?

The current EU 5G strategy sets the following objective:

"All urban areas as well as major roads and railways should have uninterrupted 5G wireless broadband coverage, starting with fully-fledged commercial service in at least one major city in each EU member state already by 2020."

5G is a global standard. The mobile industry under the auspices of the Third Generation Partnership Project (3GPP), and supported by GSMA, has worked together to specify technical parameters and protocols. 5G will enable superior performance compared to 4G in terms of speed, latency and device density.

- **Broadband Access (eMBB): 10 Gbit/s peak rate for a mobile, 100 Mbit/s average user experience, up to 1 Gbit/s under certain conditions, also a basis for 'Fixed Wireless Access' solutions**
- **Latency/reliability/availability (URLLC): 1 ms over-the-air latency, ideal for vehicle communication, remote surgery and factory automation**
- **Device density (mMTC): Support connection of device density of up to 1 million/km^2; devices which are low-cost and battery-driven, ideal for smart metering, logistics and body sensors**

A 2016 study by the Commission concluded that by 2025, the economic benefits in four sectors (transport, health care, energy and automotive) would be EUR 113 billion and 2.3 million jobs created.[24]

However, there are a few requirements to be met for 5G to achieve its full potential, both in terms of technological performance and in terms of societal and economic impact.

SPECTRUM IS KEY

5G connectivity depends on the availability of spectrum. As 5G operates on a wide range of frequencies, multiple allocation decisions by regulators and coordination amongst them are required. This is happening across the world, including in Europe. By the end of 2020, European Member States will have assigned the first blocks (primary bands) of spectrum (i.e. 700 MHz, 3.5 GHz and 26 GHz). **Unfortunately, modalities and costs of spectrum assignment are still fragmented across the EU and often represent a heavy financial burden.**

Spectrum policies are key for the success of 5G. Policies that support or even encourage technology and service neutrality (used for 2G/3G/4G and 5G) will provide operators with more flexibility to bring services to the market.

As 5G is being rolled out, and in particular with IoT and FWA scenarios in mind, more spectrum will be required, notably:

- On the C Band, we suggest prioritising national licensing to achieve national coverage and benefit the penetration.
- We recommend making use of the 3.8 – 4.2 GHz range, with national and local licensing in different parts of the band for FWA and local private networks.
- For the 26 GHz band, availability of uninterrupted 3 GHz would be preferable.
- At the World Radio Conference (WRC)-19, we suggest mobile communication identification for 37 – 43.5 and 66 GHz.
- The 6.425 – 7.125 GHz ranges should be assigned to mobile communications at WRC-23.

Besides spectrum, policy-makers and industry need to pay attention to at least two critical parameters.

5G DEPLOYMENT

The deployment of new antenna sites can be hampered by local regulation and electromagnetic field (EMF) restrictions. There are three elements creating a fact-based framework for this discussion:

- The 'International Commission on Non-Ionizing Radiation Protection' (ICNIRP[25]) developed human exposure guidelines based on a large number of scientific studies.
- Compliance standards describe the methods used to determine that exposure from antennas and mobile devices remains below the recommended exposure limits (IEC62232, IEC62209).
- Modern 5G antennas have lower power consumption than their predecessors and their design reduces the average exposure of individuals in a given area.

The mobile industry (represented by GSMA[26]), in line with the positions of the World Health Organization (WHO) and the International Telecommunication Union (ITU), has expressed support for these guidelines and standards, which the majority of Member States implement. Some Member States and even regions have nevertheless imposed specific limits taking updates of the technologies into consideration. **Going forward, we would recommend a harmonised, evidence-based approach across the EU following ICNIRP guidelines.**

Antennas are not the only deployment issue Europe must pay attention to if it wants 5G to become a success. Other key points include the following:

- 5G base stations must be linked to a fast backhaul network, preferably fibre. Policy-makers can provide tremendous help by offering financial, planning and regulatory support for fibre connections to base stations.
- Small mobiles' antennas (mainly for 26 GHz deployment) need to be exempted from prior authorisation. The consultation by the Commission and the BEREC guidelines on this topic which are under discussion are welcome contributions in this regard.

5G SECURITY

5G security has become a bigger policy issue and industry topic than 4G security has ever been. This is mainly due to the vast array of use scenarios supported by 5G networks: a wide range of applications in vertical industries, with a massive amount of connected devices. In addition, 5G will rely much more on virtualisation and cloud computing than its predecessors.

Mobile network security standards are defined by 3GPP[27] and aim to protect the network core, radio access and user devices.

They mitigate a number of security threats, including

- protecting user identity to prevent attackers from **monitoring their communications or tracking their movements**;
- providing encryption on the air interface between the user device and the base station to ensure **confidentiality of conversations or data**; and
- preventing criminals from **impersonating a user in order to obtain a service for free** through network design.

5G security standards are enhanced compared to 4G. As we outlined in our White Paper "Partnering with the industry for 5G security assurance" published in May 2019[28]:

"5G standards themselves include more security features to tackle potential security challenges and lead to security enhancements in the future 5G lifecycle."

Examples include:

- Longer encryption keys such as 256-transmission;
- ID transmission in cipher text. In 2G, 3G and 4G networks, users' permanent IDs (international mobile subscriber identities – IMSIs) are transmitted in plain text over the air interface. Attackers can exploit this vulnerability to track users. In 5G networks, users' permanent IDs are transmitted in cipher text to defend against such attacks.

5G will interconnect with other networks and technologies much more than previous mobile generations. However, it would be misleading to assume that the only protection measures applied to interconnecting networks are the 3GPP security standards. The applications and edge network functions running over the 5G networks need their own security.

We need a multi-layer security architecture and to focus on end-to-end protection. Partnerships – as recommended in the Huawei White Paper quoted above – between different operators, software vendors, equipment producers and industrial stakeholders going beyond the boundaries of the mobile industry play a key role in delivering a secure 5G ecosystem.

We should also keep in mind that several 3GPP security standards are optional. They could be made mandatory and their implementation audited by national telecom regulators. A Europe-wide scheme could harmonise these requirements.

The Commission has launched a process to find a coordinated security response across the EU. Member States are requested to inform each other on their envisaged national approach. On this basis, the Commission – supported by ENISA – intends to make appropriate policy proposals towards the end of 2019[29].

We welcome this approach and recommend focusing on a holistic, cross-industry approach and close cooperation between private and public stakeholders. Considering the wide range of stakeholders involved, a set of voluntary and/or mandatory security certification schemes would be a sensible measure. To be effective, they should be linked to respective audit processes.

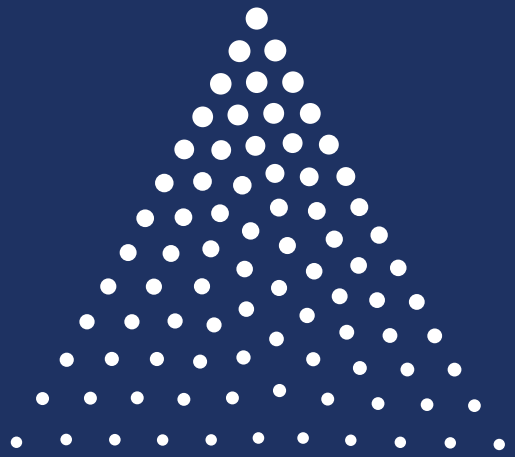
All of this will help, in particular to raise awareness, build trust and thereby trigger investments. However, it is important to consider security as an ongoing, open-ended process of constant improvement (see chapter 10).

OUTLOOK

5G equipment is provided by a number of vendors, deployed and managed by operators, and augmented by industrial applications. This requires an open and investment-friendly environment. 5G security is a priority and a concern not only for the mobile industry but also for other industrial stakeholders.

A policy environment supporting the deployment of 5G networks, in particular by addressing spectrum conditions, deployment restrictions and public investment opportunities, and by fostering an industry-wide, rational security approach will make a key contribution to making 5G work for Europe as a whole.

6



6. TELECOM OPERATORS: EUROPE'S UNDERESTIMATED ASSETS

Europe is identifying strategies to gain more ground and leadership in the digital world. Europe typically has strong research resources but lacks actors transforming these into business growth. The obvious question is why Europe is not paying more attention to one of its biggest assets: telecom operators.

As Telecom Italia CTIO Elisabetta Romano put it: ***"Regulators must step in to help pull Italy's telecoms industry out of a negative spiral of severe price pressure. … The regulator has a lot of work and a big responsibility to look at the industry and compare with other industries. To do some sort of post-mortem as to what has happened in the last ten years and try to understand how they can help."***[30]

HOW DID WE GET HERE?

Since the first comprehensive telecom liberalisation package in 1998, former state monopolies have been transformed into private operators listed on stock markets (some with shares still owned by the government) and, most importantly, have become subject to competition.

During the ten-year period between 1995 and 2005, technologies advanced rapidly: 2G (GSM) became a stunning success, and the number of internet users grew exponentially, ADSL and DOCSIS offered broadband connectivity on phone lines and coax cables, while local loop unbundling intensified competition. All this created a positive momentum with the expectation being to see thriving European operators compete on par with US operators.

Unfortunately, these expectations were not fully met, and this for mainly two reasons. Firstly, the auctioning of 3G (UMTS) spectrum turned out to be a big success for Europe's finance ministers but a disaster for telecom operators. The negative consequences can still be felt today in the market. Secondly, the world turned to the internet (TCP/IP) as the preferred communication platform (protocols) for digital services. In the internet world, telecom networks route packets but do not manage the services delivered by those packets, a fundamental shift for operators.

Net neutrality rules ensure that everyone can offer services to everyone connected to the internet. The internet has undoubtedly become a dominant factor in the lives of billions of people and has created a huge digital economy. It has also given rise to new global, mainly US and recently Chinese, players, something which did not happen in Europe. Where does this leave the European telecom operators?

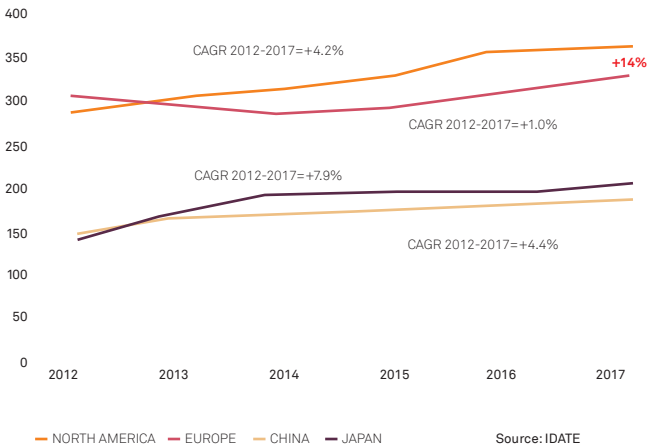
OVERCOMING STRUCTURAL CHALLENGES

Telecom operators face structural problems. Over time, growth of operational costs (OPEX) has been larger than their revenue growth. IDATE notes: ***"Subscriber numbers and thus overall revenues are continually growing, albeit slowly, but the revenue generated per subscriber is decreasing, while EBITDA continues to be squeezed and CapEx spending obligations increase. European telcos in particular are having a hard time, with both internal competition (against other telcos) and external competition (against OTTs) taking its toll."***

IDATE, 'KPIs: Telcos vs OTTs, How internet giants differ from telcos', 5 June 2017

Over the 2008-2017 period, retail telecom service revenue decreased by 12% in Europe while revenue grew by 13% at global level (+8% in the USA), with a similar picture emerging when only looking at the last 5 years to exclude the period of the financial crisis.

TELCOS REVENUES BY NATIONAL CLUSTERS (BILLION EUR)



Some of the structural problems are global, but European operators seem to be particularly affected: American operators perform much better than the rest of the advanced economies. Asian companies are growing fast. European operators keep suffering losses.

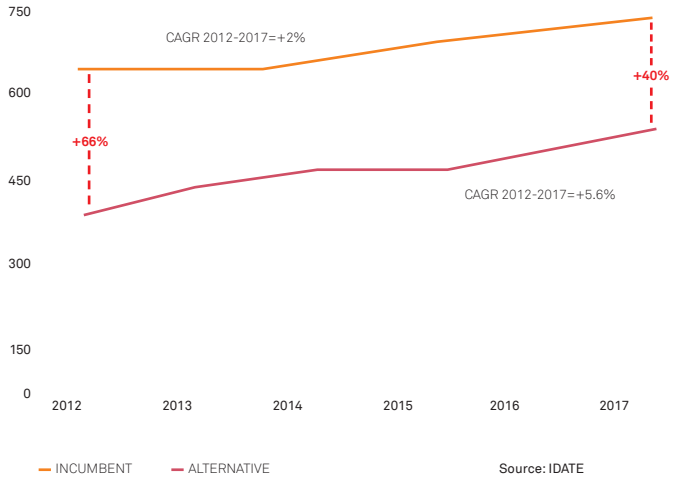
It is evident that the (monopoly) copper network had to be opened up to competitors through ex-ante regulation. It is less evident that the same type of regulation should apply to new networks, in particular investments in fibre networks. As (fixed) networks tend to be natural monopolies, there is still a rationale for regulation, but does it have to be the same detailed, ex-ante regulation as 20 years before?

A POLICY CHANGE IS NEEDED

The US and Asia (in particular China, Japan, South Korea) have strong global players in the internet economy and IT equipment, and also big telecom companies. European policy-makers often ask the question of why Europe does not have these kinds of companies. What could help European telecom operators to play a stronger global role?

This should start with a **change in perception**. The days of monopolies are over, with the average share of new entrants in broadband delivery being about 60% in 2018. New entrants' revenue growth has been larger than that of incumbents: the gap is closing.

REVENUES FOR TELCOS BY 'INCUMBENT AND ALTERNATIVE' CLUSTER (BILLION EUR)



Another point is **investments**, where we can see a paradox. European operators invest relatively more than their global counterparts, taking the capital spending to turnover ratio as a measure point. Yet, IDATE estimates a EUR 50 billion annual investment gap when compared with the US because of much lower revenues. This is keeping Europe's telecom sector in a low profit and low investment cycle.[31]

In the same way, the European Investment Bank has estimated the investment gap between 2020 and 2025 at EUR 250 billion.[32]

In the past, there has been a strong focus on consumers' and citizens' benefits, which is an important consideration, yet the pendulum has swung too far. We would advocate including an element in the digital strategy which **focuses on the capability of the European telecom sector to invest.**

OUTLOOK

The fibre network roll-out (chapter 4) and 5G deployment (chapter 5) would both be crucial elements of such a policy. For instance, applying 5G to industry applications, i.e. exploiting its short latency and massive machine-to-machine capabilities, requires additional investments (for instance in mobile edge computing, additional base stations, and a performing network core) and partnerships. This looks like a perfect case for significant action, maybe even a 'mission', under Horizon Europe.

The coming years will see the implementation of the 'Code'. The national regulators and BEREC will play a key role in this context. They should use their regulatory flexibility to reduce the regulatory burden as much as possible. A review of the Code would be premature, but some targeted improvements could be envisaged, even ahead of the scheduled evaluation in 2025.

A very concrete example is the new "wholesale only" model that is proposed as a regulatory option in the Code. European regulators need to make sure that setting up this model would not lead to reduced investments because of lower incentives. This could also lead to value destruction among retail services providers which will only be able to differentiate themselves through pricing and not through innovation enabled by infrastructure.

Telecom policy has become predominantly aimed at safeguarding service competition and public interests, and keeping consumer prices low. Industry policy aspects such as innovation capability, investment levels and the role of European operators in the world have moved out of focus.

At a time of dominance of the big internet players, Europe could consider a more pro-active approach in favour of one of its key assets, telecom operators. There is no need for protectionism, but rather less regulation, more affordable spectrum, promotion of industry partnerships, and support for 5G deployment.

This would create an environment that allows operators to deploy state of the art infrastructure and service innovations with significant spill-over effects, for instance nurturing European start-ups. It would also equip operators with a financial capacity to offer service innovation at a global scale.

7. SMART CITIES: WHY DOES IT TAKE SO LONG?

The notion of a 'smart city' refers to the use of digital technologies to make them more efficient, convenient and sustainable. Cities across the world have taken action to become cleaner, safer and less polluted with the help of digital technologies. Progress has been made. Yet, we are just at the beginning.

Today, many cities offer online access to information and services through the web and increasingly on smartphones via city apps targeting specific areas (tourism, traffic, public administration, public transport schedules...).[33] However, the aspirations of what smart cities could achieve go much further.

For instance, a McKinsey analysis[34] showed the potential benefits generated by smart city applications: They could

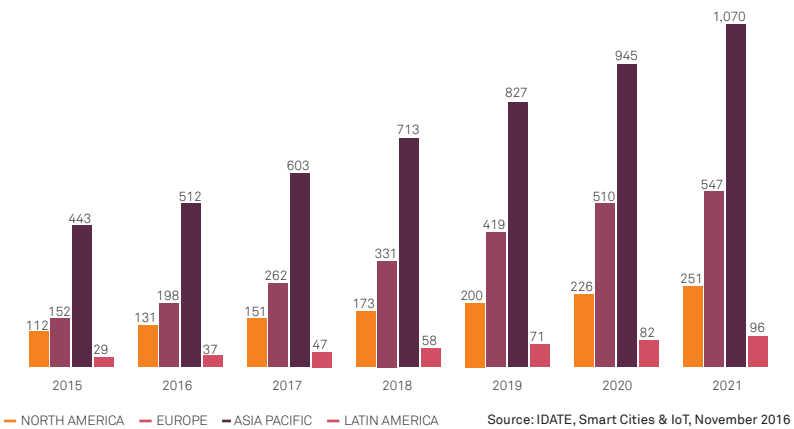
- reduce fatalities by 8–10%;
- speed up emergency response times by 20–35%;
- shave 15–20% off the average commute;
- reduce crime by 30–40%;
- save 25–80 litres of water per person per day; and
- cut greenhouse gas emissions by 10–15%.

In order to realise these benefits, a comprehensive approach is needed, covering all layers that need to interact.

City management platform: cloud-based integration of siloed information, automation of decisions, one-stop-shop services, data analysis
Applications layer: mobility, environment, safety, energy, governance
Data layer: collection, generation, labelling, organisation, storage
Connectivity layer: mobile and fixed networks
Device layer: smartphones, sensors, cameras

When looking at the available case studies and deployment data, we can see that most of the initiatives can still be considered projects. Deployments on a city-wide scale with considerable investments are still the exception. Cities in Asia and the Middle East are pushing ahead with life-changing infrastructure projects, such as Yanbu (Saudi Arabia), Weifang, Shenzhen and Dunhuang (China) and Singapore. Europe is lagging behind.

NUMBER OF CONNECTED OBJECTS DEPLOYED BY REGION, 2015-2021 (IN MILLION)



Source: IDATE, Smart Cities & IoT, November 2016

BARRIERS TO DEPLOYMENT

What is holding smart cities back? In essence, three things: mindset, money and management.

- **Mindset:** a comprehensive smart city concept is a political challenge as it requires substantial investments. It requires the willingness to re-think how the administration works and to overcome silo practices, for instance to establish a data (sharing) strategy, implement automatic decision-making supported by AI, and integrate service provision. Cities need to be open for private sector investors without losing their focus on citizen welfare.
- **Money:** deploying smart solutions offers multiple opportunities for cost savings and better services, but the return on investment is not obvious. How can private investors make money without destroying the infrastructure paradigm? City management must be able to demonstrate that the solutions are sustainable.
- **Management:** smart city initiatives require advanced project management capabilities to ensure timely delivery and cost control. Migrating legacy infrastructure to an integrated and interconnected platform can be very complex and requires the collaboration of many stakeholders. The risk profile can be such that cities shy away from entering into a comprehensive deployment phase and remain at the level of individual pilot projects.

HOW DO WE RESOLVE UNDER-INVESTMENT IN SMART CITIES?

To overcome these obstacles, cities need to work together. This is already happening within the framework of city associations. For instance, the Eurocities network[35] provides a collaborative framework for tackling some of the challenges cities are facing.

Smart cities should not be technology-driven in the first place: the concept should revolve around people and their lives. It is about how to make better decisions, solve problems and improve quality of life. Of course, city management also requires awareness of what is technologically feasible – whilst not every fancy technology needs to be deployed. As Smart Cities solution architect Radim Cmar explains in an article[36]:

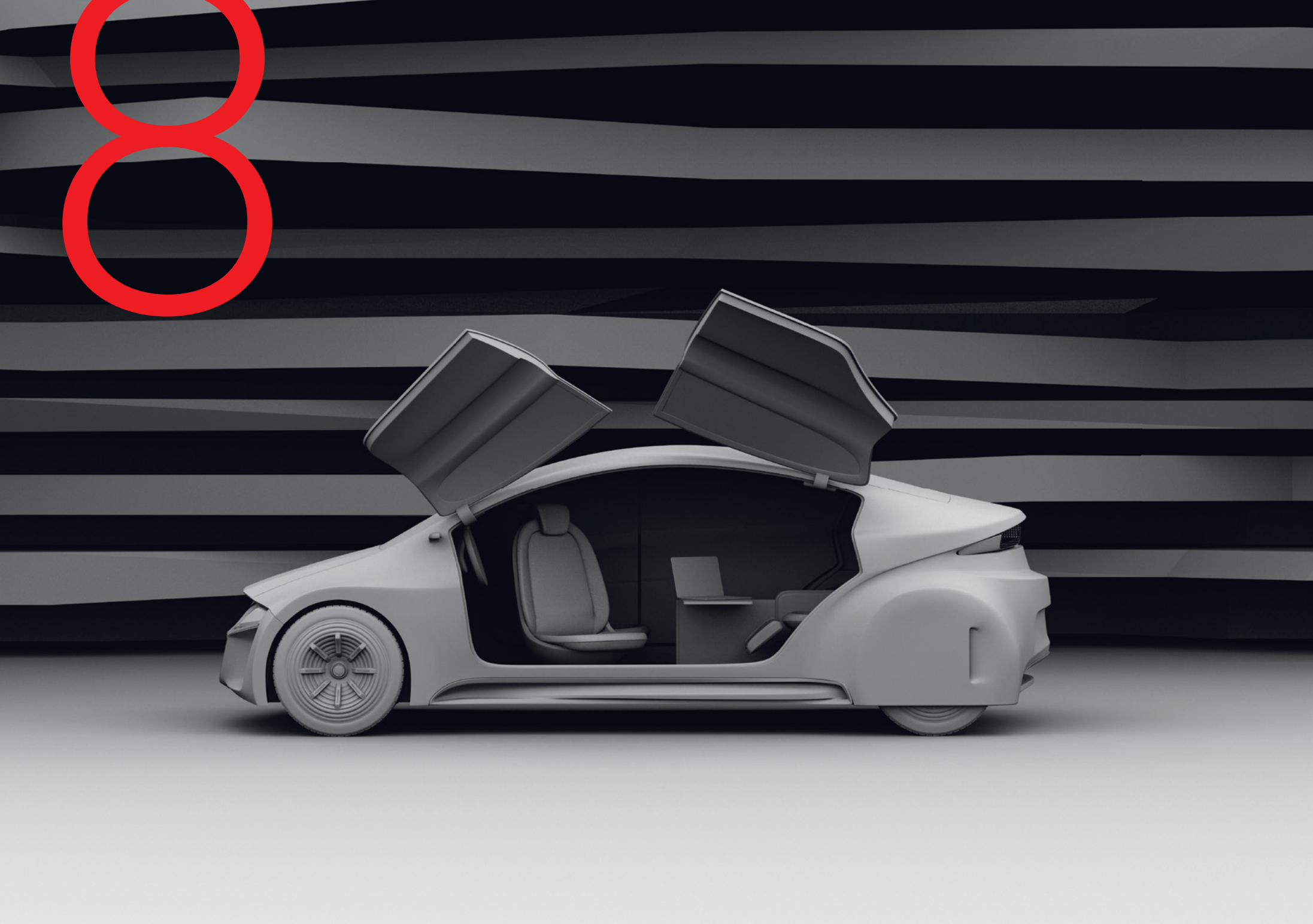
"Solutions need to come from cooperation with the city, starting with pilot programmes wherever possible. As the solution evolves, the city must be open to listening to citizen feedback and committed to iterative improvements."

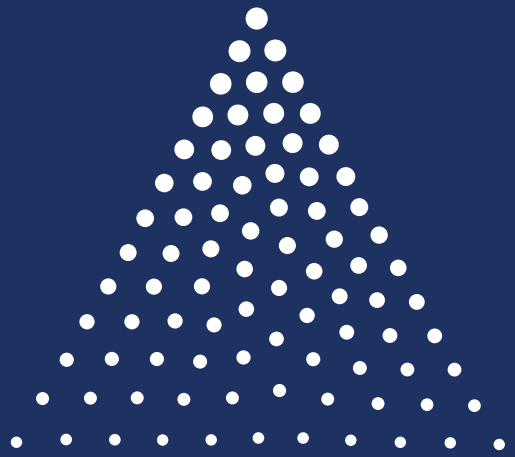
Europe needs a comprehensive smart city investment programme. The proposal of the Commission for a Digital Europe programme is technology-driven with deployment of AI, cyber security and quantum computing as focal points. The envisaged concept of 'missions' as part of Horizon Europe, including smart cities, could already make a difference. However, a much bigger and bolder initiative would be required, involving national budgets. What we are talking about is a comprehensive investment framework, including all funds with a vision and targets. For instance, 5G deployment and smart city investments could go hand-in-hand. Europe should set ambitious targets such as aiming for 100 'real' smart cities in Europe by 2025.

OUTLOOK

To unleash the full potential of digital technologies, cities need to move beyond the isolated deployment of technologies and towards interconnected infrastructure and data serving multiple purposes. More public-private partnerships would help. Europe could create an overarching policy framework, including Member States' initiatives, for delivering a strategic vision. This should include an ambitious programme to make the necessary financial resources available.

8





8. CONNECTED MOBILITY: ARE WE READY FOR A BIG MOVE?

A NEW PARADIGM IS EMERGING

The car industry is preparing for its biggest transformation yet. Electrification, self-driving cars, in-car and smartphone-based navigation systems and the proliferation of ride-hailing and sharing services are leading to a paradigm shift.

Cars are already equipped with many on-board sensors, radar equipment and cameras, making driving safer. While these solutions are valuable, they have limitations. For instance, 80% of car accidents could be prevented with enhanced vehicle connectivity. V2X *(Vehicle to Everything)* technology will remove these limitations to a large degree. There are two main communication technologies which are ready for the market. One technology is based on the Wi-Fi protocol (IEEE 801.11p – also known as DSRC or ITS-G5), the other one is based on cellular communication – 4G and in the near future 5G (C-V2X). Both operate on the 5.9 GHz band and are not interoperable.

There are industrial supporters for each[37]. Huawei firmly believes that cellular technology is superior in performance, and in particular 5G will bring connected car services to an unprecedented level. It is true that DSRC has been piloted for a longer period than cellular, but C-V2X is now ready for deployment too. **Therefore, our recommendation is to invest in future-proof technology and for the regulators to stay neutral.** Europe should be consistent: If 5G is a priority then C-V2X should not be excluded by regulators.

THE FOURS STRANDS OF VEHICLE-TO-EVERYTHING COMMUNICATION

- **C-V2V (Vehicle to Vehicle):** short range car-to-car communication which works without network and wide-range communication using a mobile network. This enables forward-looking information about dangerous situations (accidents, traffic jams, road hazards, broken down vehicle) being communicated backwards from cars ahead. It allows drivers or cars, as it were, to coordinate movements or alert each other about changes of direction. A network connection would allow this alert mechanism to function many more kilometres ahead.
- **C-V2P (Vehicle to Pedestrians):** modern sensors and modems will enable awareness of and communications with pedestrians, road maintenance personnel and cyclists, thereby being able to react (brake) faster and warn the so-called 'vulnerable road users' about potential danger.
- **C-V2I (Vehicle to Infrastructure):** when cars and road infrastructure such as traffic lights, signs and cameras are enabled to communicate with each other, safety and driving experience improve. The infrastructure becomes an active part of real-time traffic management, for instance by collecting information on traffic and road conditions.
- **C-V2N (Vehicle to Network):** mobile networks underpin the services and information flows mentioned above. In addition, they connect individuals, for instance through on-board systems and smartphone apps, to a wider set of services, such as parking guidance and individual routing recommendations. Mobile networks will connect the car system to cloud services providing predictive car maintenance. V2N will naturally deliver entertainment and office worker support services.

Whilst the performance of C-V2X will improve rapidly, autonomous driving as such will not depend on connectivity. As the name says, a self-driving car must be autonomous. However, traffic will be safer, smoother and more efficient with a well-performing C-V2X infrastructure. For instance, the intelligence gathered by road infrastructure (using cloud-based services) and transmitted via mobile networks can control traffic flow, velocities and inter-vehicle distances based on this information.

This symbiosis of technologies enabling self-driving cars and supporting C-V2X connectivity will both require and generate changes in legal provisions (e.g. liability), transport policies, city management, and business models of the automobile industry at large. It will also have an impact on consumer perceptions and behaviour. For instance, the propensity for car ownership could (and most probably will) shrink while ride-hailing businesses and car-sharing could flourish. Public transport could be better interlinked with individual movements and become more attractive.

Policy-makers actively support these changes and foster related innovations because they promise to solve a number of transport-related problems.

FINDINGS PUBLISHED BY THE EUROPEAN COMMISSION IN 2017[38]

- 25,500 deaths on EU roads in 2016, 38% in urban areas
- 135,000 seriously injured
- Human error is key source of accidents in transport
- Traffic congestion costs an estimated EUR 80 billion every year
- Urban areas account for 23% of all CO_2 emissions from transport

The EU's overarching policy objective is to achieve a cleaner, safer and more efficient transport system in the EU. This was set out most recently in the Commission's Third Mobility Package of 17 May 2018[39]. As part of this package, the Commission published a strategy to make Europe a world leader in fully automated and connected mobility systems.

HOW DO WE GET IT DONE?

Many actors are involved, but who will fund V2X deployment? Some services should be provided for free, for instance safety- related information, and fall into the remit of public infrastructure. Tendering and procurement of road infrastructure are governed by strict and detailed procedures and operate in cycles of five to ten years, which is somewhat at odds when confronted with fast-moving technologies.

Regarding paid services, we are in a 'chicken and egg' situation: V2X needs high investment and has considerable operation costs, but there will be no significant revenue before achieving a high penetration. V2X equipment vendors and network operators need to collaborate with vehicle manufacturers to agree on functionalities and standards.

The current approach of technology support (e.g. as part of H2020) on the one hand and transport policy (e.g. ITS Directive) on the other could be enhanced by a 'Master Plan'. There are many parameters which depend on each other to manage, thus strategic coordination appears necessary.

OUTLOOK

The emergence of connected cars, autonomous driving and innovative mobility services, along with electrification of vehicles and massive data availability coupled with AI, will change the way people travel and freight transport is managed. The contribution to EU mobility objectives will be significant, in terms of safety, efficiency and the environment (de-carbonisation).

The EU mobility strategy needs a decisive implementation agenda which goes beyond transport-related issues. We call it a 'Master Plan' which would address joined-up infrastructure and car equipment deployment. This would be a real big move.

9. ARTIFICIAL INTELLIGENCE: IS IT REALLY A GLOBAL RACE?

At first glance, the answer is yes. After all, both the US and China have announced their ambitions of becoming 'the' global leader. Both, indeed, lead the world in almost every yardstick of progress in AI, in particular with regard to investments, market size and number of top companies. Policy-makers in Europe want to lead with 'responsible, ethical AI'. Several nations such as Japan and India have also published strategies with ambitious goals.

Yet, a race is about winning and losing and here things are becoming more complex than the simple notion of a 'race' between nations seems to suggest. As pointed out by Paul Krugman, Nobel Prize winner in economics, *"companies compete, not countries"*. Companies compete globally for market share and aim to make profits for shareholders. They do not compete for the sake of national objectives. Of course, countries would like to headquarter as many successful companies as possible, but this does not create a win-lose situation. For instance, by using US or China-based world leaders in AI, a European company in a vertical industry can gain an edge vis-à-vis its competitors from the US or China. Therefore, global progress in AI benefits everybody and offers opportunities for all.

"The responsible development and use of Artificial Intelligence (AI) can be a driving force to help advance the SDGs and to realize a sustainable and inclusive society. To foster public trust and confidence in AI technologies and fully realize their potential, we commit to a human-centered approach to AI, and welcome the non-binding G20 AI Principles, drawn from the Organization for Economic Cooperation and Development (OECD) Recommendation on AI."

G20 Osaka Leaders' Declaration

Analysts such as PricewaterhouseCoopers and McKinsey estimate that AI could contribute up to USD 13-15 trillion to global GDP by 2030. This impact is much bigger than AI technology markets as such, i.e. software, services and hardware (including public cloud usage), which as of 2018 represented around USD 60 billion worldwide and are expected to grow to USD 800 billion by 2025 (estimates based on Tractica analysis). From a macro-economic point of view, what matters is the widespread and efficient use of AI across all sectors.

Keeping pace with the extraordinary speed and depth of AI development over recent years is a challenge for policy-makers. Scientific papers, patent statistics and data on start-ups and researchers provide extensive evidence of this.

AI DEVELOPMENT IN FIGURES[40]

Scientific publications on AI

1.6+ million

since the inception of AI in the 1950s
Leaders by number of publications:
Worldwide

1. EU

1. UK
2. Germany
3. France

2. China

Rapid increase in global share:
3% in 1997→ 27.7% in 2017

3. USA

AI-related inventions

340,000
AI patent applications since the 1950s

More than **50%** since 2013
Leaders by application filings:
USA, China & Japan
(1997-2017)

Deep learning:
175%
Average annual growth of applications

→ Biggest recent growth
Average rate for all technologies:
10%

Successful international collaboration

23.4%
is cross-border teamwork

Highly cited papers:
42.6%

AI start-ups

USD 50+ billion globally

invested in AI start-ups between 2011 and mid-2018

2/3

of the total from the USA

USA

Average size of investment:

2016 USD 9.5 million ↗

First half of 2018 USD 32 million

Largest deal: self-driving car start-up Zoox

USD 500 million

China

3% of start-up investments in 2015

↗↗

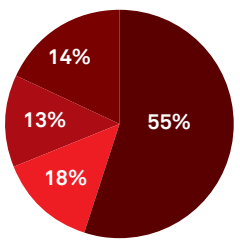
36% in 2017

EU

1% in 2013 ↗ 8% in 2017

→ lagging behind

COUNTRY SHARES OF EU PRIVATE AI START-UP INVESTMENT (2011-2018)



- UK **55%**
- GERMANY **14%**
- FRANCE **13%**
- REMAINING 25 COUNTRIES **18%**

AI researchers

INTERNATIONAL RANKING

Number of researchers with issued patents and/or published English papers over the last 10 years

EU (5) 33,516 (16.3%)

Germany **9,441 (4.6%)**
UK **7,998 (3.9%)**
France **6,395 (3.1%)**
Spain **4,942 (2.4%)**
Italy **4,740 (2.3%)**

USA 28,536 (13.9%)

China 18,232 (8.9%)

India 17,384 (8.5%)

A EUROPEAN AI AGENDA

In 2019, the European Commission adopted its Action Plan on AI[41], setting up, inter alia, a High-Level Expert Group[42] which has issued a long list of recommendations. Many organisations, for instance the OECD[43] and most recently the G20[44], have published guidance on what a supportive AI policy could entail. Amongst the many recommendations, we have singled out four areas which deserve specific policy attention in a European context:

1. ATTITUDE

Europe has a lot of talent, but fewer start-ups, and in particular big ones, than the US and China. While access to venture capital has been identified as the main reason, the bigger picture appears to be the generally sceptical attitude in Europe towards disruptive technologies in the Schumpeterian sense. As the venture capitalist Kai-Fu Lee describes in his book "AI Superpowers", a frenzy of enthusiasm broke out in China after Deep Mind's AI beat the world champion in Go, stimulating start-ups and entrepreneurship even more. This is a far cry from the European mindset.

European policy-makers need to focus more on fostering optimism and entrepreneurial spirit. They should demonstrate the potential for society (for instance better health care, education and environmental protection, as presented by the World Economic Forum[45]) and steer the sometimes irrational discussion towards an evidence-based one. Progress on these counts will be difficult to measure, but decisive for the outcome.[46]

2. IMPLEMENTATION OF REGULATION

Market regulation at its core is a trade-off between business freedom and protection of general interest. The General Data Protection Regulation (GDPR) reflects European values and, without targeting AI specifically, creates a framework for dealing with private data. The GDPR imposes a number of obligations which are for good reasons not technically defined. The challenge is that companies, in particular smaller companies, must figure out whether a certain AI implementation is in line with privacy regulation.

European regulators could do more to help companies, in particular small firms and start-ups, to overcome such regulatory uncertainty. The regulatory burden – in areas related to GDPR and beyond – must be reduced, for instance by developing adequate standards and certifications of technical solutions so that private actors obtain assurances and understand what it takes to be compliant.

3. VERTICAL INDUSTRIES

AI will be applied across the entire spectrum of the economy, including in the public sector. Implementation of AI (e.g. collaborative AI robots, cognitive AI systems) needs a data strategy and a holistic transformation of traditional business models. This is quite natural for the big American and Chinese internet players which are all data-driven. It is more of a challenge for companies from other sectors. Therefore, promotion of AI amongst a wide range of industries with a focus on smaller and medium-sized companies should become a policy priority. Europe should pay attention to diversifying the use of cloud-based AI platforms beyond the global leaders. Policy-makers could for instance support AI platforms in cooperation with European telecom operators.

4. ETHICS

The Commission has set up an expert group which issued a catalogue of guidelines. The OECD has also published work on it[47]. Similarly, the G20 conclusions refer to common principles regarding AI[48]. Individual countries such as the UK, France and Germany are doing the same. They all point in the same direction, e.g. transparency and explainability, preparation of workers for a new environment, and respect for privacy.

What matters is implementation. Agreeing on principles is one thing, putting them into action is the real challenge. Whilst some of the issues are already covered by regulation, for instance by the GDPR, policy-makers will need to tackle unprecedented aspects, such as so-called 'deep fake videos' and 'automatic decision-making'.

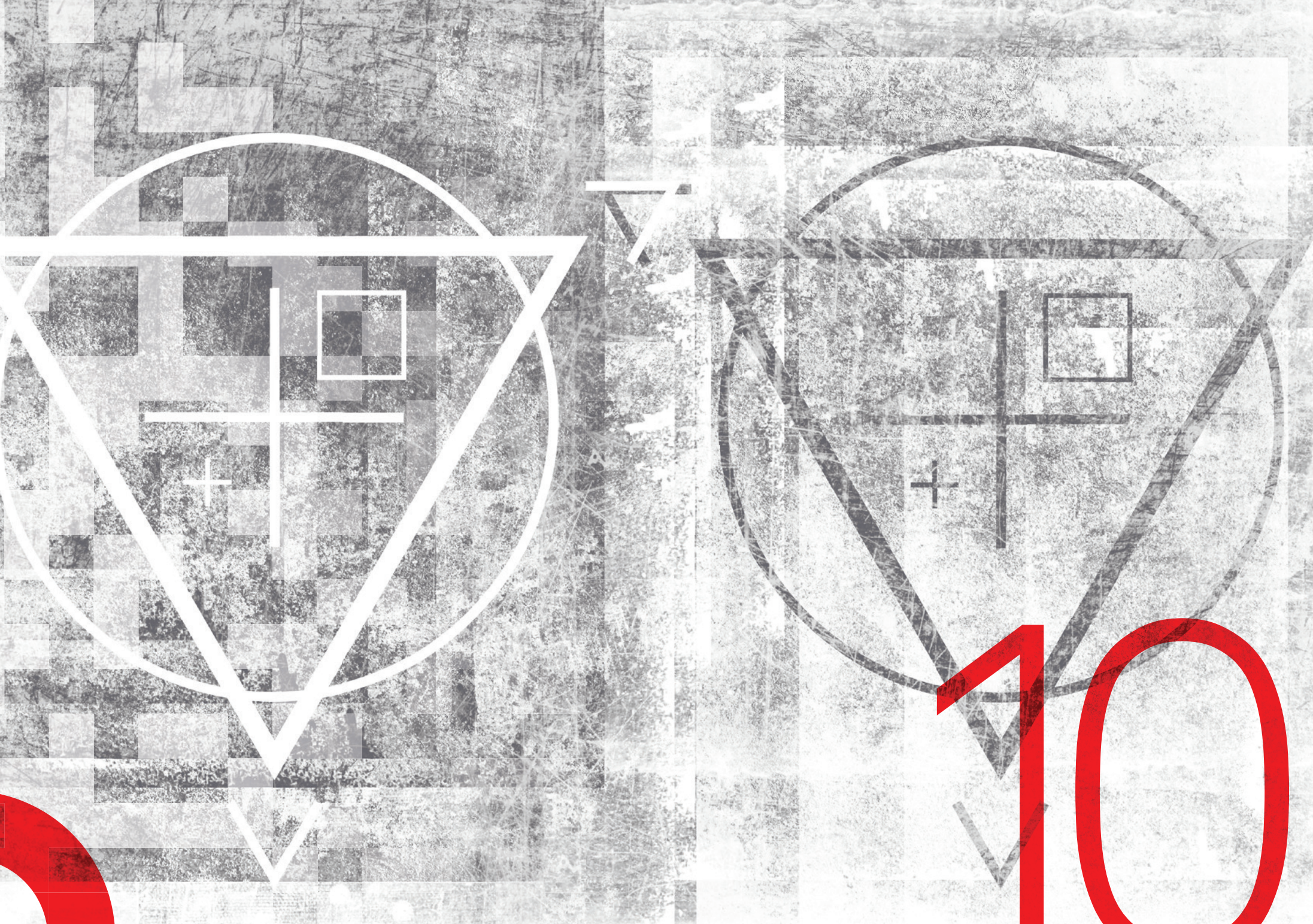
With the impressive progress in AI-generated videos (with decreasing needs for large data sets), the potential danger of widespread abuse of fake videos which are hard to distinguish from authentic ones is real. Platforms that make AI video tools available and social media that distribute videos should provide manipulation detection measures, preferably easy-to-use ones. We also need to tackle skills, e.g. we need more real-life training on media forensic tools for journalists, investigators and other professionals.

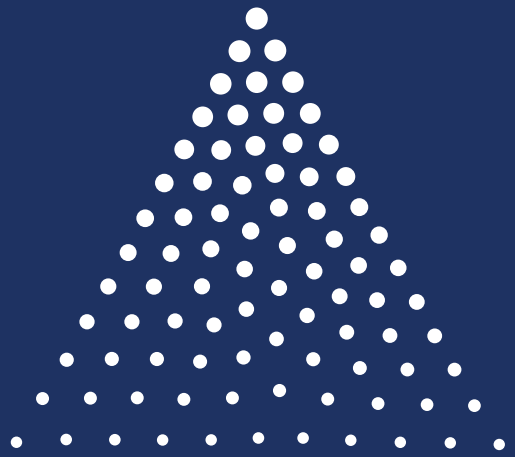
AI can be used to automate processes. Some applications should not raise any concerns. In telecommunications for instance, this capability can be used to improve network performances. In manufacturing, predictive maintenance can be improved. Some applications, however, for instance hiring decisions, university admissions and determining insurance premiums, affect people's lives directly so the need for transparency and non-discrimination is much higher.

OUTLOOK

There is overwhelming agreement that the impact of AI on the economy and society will be huge. AI technologies develop at a rapid pace. Whilst it is true that industry players in the US and China have a lead, there is strong potential in Europe in terms of talent, research and industry capabilities. Europe should take advantage of it by embracing the opportunities offered by the global AI industry and build local capacities also with the help of investments from international companies.

Most countries and organisations have recognised the importance of ethical standards in this context. In view of challenges such as automatic decision-making and fake videos/audio, regulation might be necessary. Any regulation will need to address the global character of AI technology and related industries and its amazing rate of progress. Broad partnership is the best way forward and will help European companies to take advantage of this transformative technology.


10



10. THE NEVER-ENDING STORY OF CYBER SECURITY: WHO WRITES THE SCRIPT?

BACK TO THE FUTURE

In 1972, researcher Bob Thomson wrote a code disseminating the message “I am the Creeper, catch me if you can” on the ARPANET. The concept of a computer virus was born.

Pioneering computer programmer Ray Tomlinson wrote a programme chasing and deleting Creeper code. The first Anti-Virus software was born.

These were academic experiments. It took the popularity of the internet, more precisely the World Wide Web, to turn this concept into a global threat.[49]

Computer security has always been a matter of concern, even before the internet age. However, with the penetration of computers in all aspects of our lives and businesses, it has become a matter of survival and a political priority. The openness of the internet, together with computer architecture, has been a recipe for success, but also created opportunities for hackers. The more penetration increases, the more is at stake, and the bigger the incentives for criminals to exploit weak points become.

A recent example is the WannaCry virus, which encrypted data on unprotected computers, making access to them impossible unless the victim paid a ransom to obtain the decryption key. Within 24 hours, it had infected more than 230,000 computers in over 150 countries.

This example demonstrates that cyber security is a distributed challenge. There are only a few centralised internet targets, for instance the Domain Name System, but a huge number of online computers and connected networks. The security tasks are not only the responsibility of operators and vendors but lie with everyone who connects their computers to the internet.

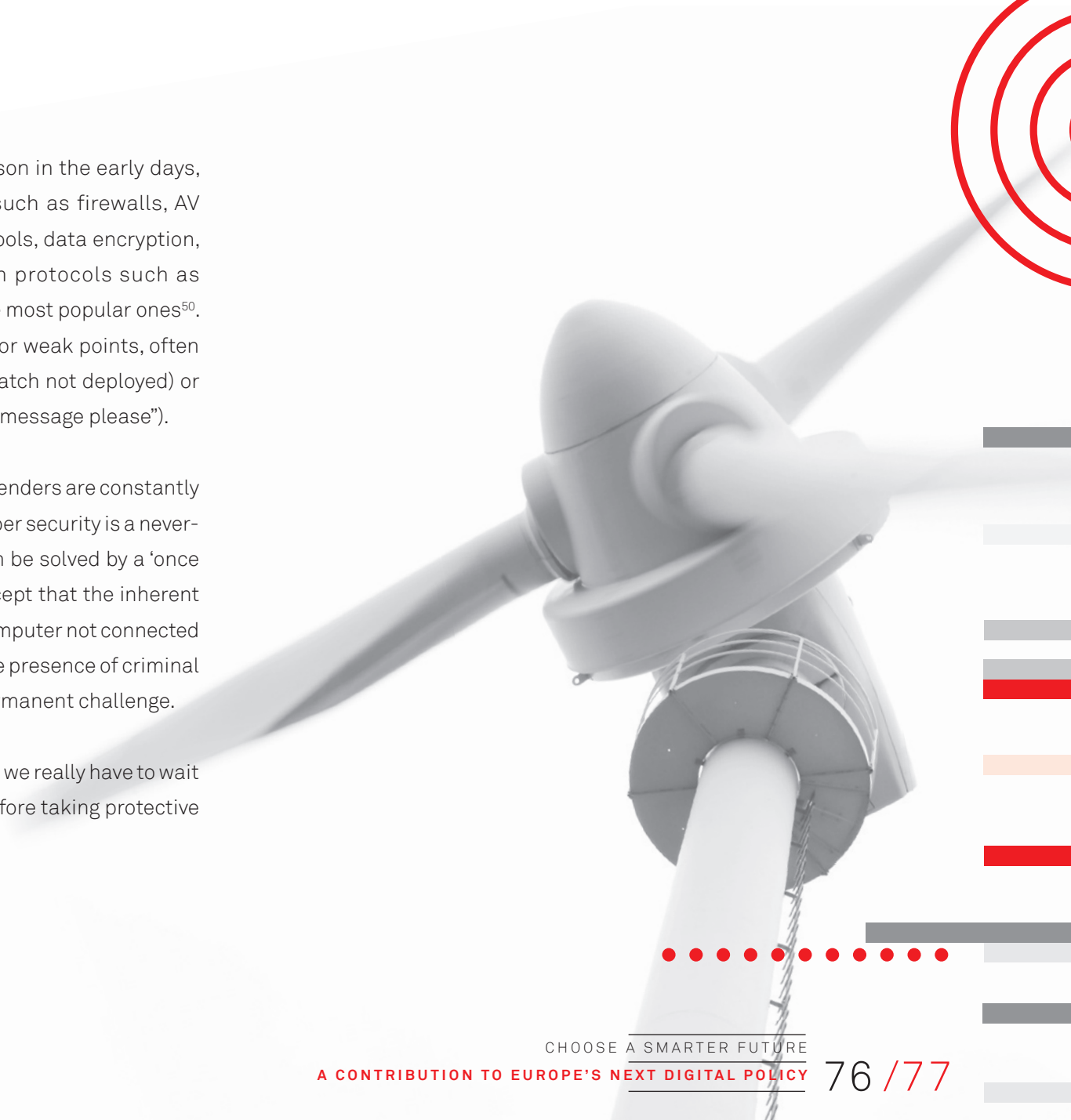
Often hackers exploit a vulnerability which – as was the case with WannaCry – has already been fixed, but many computers remain vulnerable as users fail to deploy the ‘patch’ that would protect against the virus.

For business, even more critical are hidden attacks which do not make headlines. Sophisticated, carefully crafted and dissimulated infiltration of company networks is a tremendous threat.

Cyber security experts, like Ray Tomlinson in the early days, have worked on protection methods such as firewalls, AV software, network intrusion detection tools, data encryption, access control measures, encryption protocols such as SSL/TLS and IPsec, to name some of the most popular ones[50]. However, attackers are always looking for weak points, often found in sloppy system management (patch not deployed) or human social engineering ("click on this message please").

Today, we are in a situation where the defenders are constantly confronted with new attack methods. Cyber security is a never-ending story. It is not a problem that can be solved by a 'once and for all' security design. We must accept that the inherent openness of our ICT infrastructure – a computer not connected to the internet is not very useful – and the presence of criminal intentions will make cyber security a permanent challenge.

But who writes the script of this story? Do we really have to wait for the next attack method to emerge before taking protective measures?



WE NEED BETTER SCRIPT WRITERS

In the age of the IoT and 5G, cyber security is becoming a more pressing issue. We will rely even more on computers and networks, for instance for autonomous systems and driving, robots, medical data and certification. Getting ahead of the curve would mean breaking out of the cat-and-mouse game between hackers and defenders, between computer viruses and anti-virus programmes. The principle of anti-virus and other protection mechanisms is to detect, protect and if needed recover from a list of known attacks. Can we design systems that render whole classes of attacks much less successful or even impossible? The opportunity could arise with the interconnected deployments of IoT and 5G systems. **Novel security design for network architecture and system protection could bring protection to a new level.** Let us work together on this.

AI provides another challenge and opportunity. It can help to detect unknown attacks, make autonomous decisions on how to protect and provide recommendations. AI can also be used by attackers. In one case, cyber defence company 'Darktrace' identified malware "where the attacker was using a hearing, an understanding methodology to try and understand what the network was like". Without any doubt, AI-driven attacks will occur at a large scale. **Massive anti-AI-attack research will be required to enable the industry to write that part of the script.**[51]

The industry and the research community are trying hard to get ahead of the curve. The nut to crack is to protect networks and computers without making them impractical or too costly to use. This is a trap policy-makers too often fall into. For instance, the complicated provisions for a digital signature for public services such as tax declarations have made its use unattractive in some countries. Deploying security measures without usability in mind can lead to more insecurity as users will tend to ignore or work around them.

EU ACTIONS TO STEP UP CYBER SECURITY: STATE OF PLAY

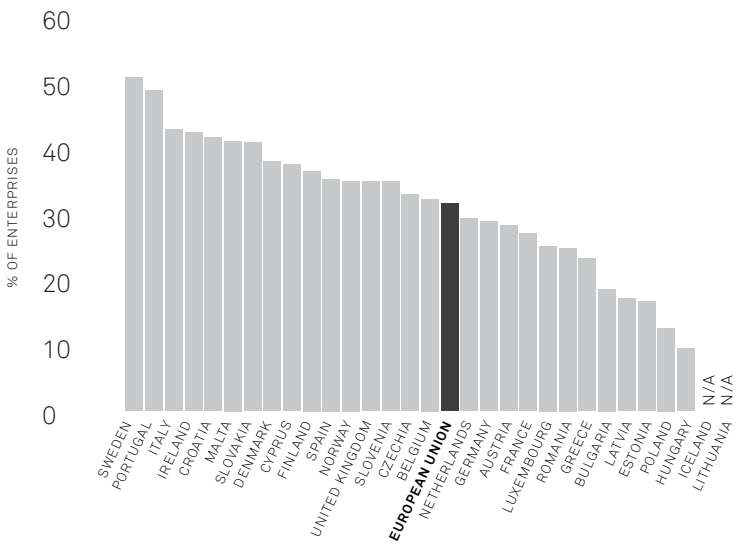
At EU level, the regulatory framework consists primarily of the Cybersecurity Act (reinforcing the role of ENISA, framework for certification), the Network and Information Security (NIS) Directive (capacity building, critical infrastructure), and the eIDAS (electronic identification, authentication and trust services) Regulation.

There is also a proposal for a 'European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres' which is supposed to manage the cyber security budget of the Digital Europe programme.

A Horizon 2020 contractual public-private-partnership, European Cyber Security Organisation[52], is also a feature.

This framework is complemented by the work of ENISA.

ENTERPRISES WITH A FORMALLY DEFINED ICT SECURITY POLICY
YEAR: 2015



SOURCE DATASET: EUROPEAN COMMISSION, DIGITAL SCOREBOARD

WHERE DO WE GO FROM HERE?

Where does this lead us for the coming five to ten years? Which policy response would help the good side to write the script?

Awareness is needed, given for instance the relatively low number of formalised cyber security policies at enterprise level: This is in particular a problem for smaller business. The 'British Standards Institutions' (BSI) points to the gap between 'need' and 'action' and recommends: "Your cyber security policy doesn't need to be very long; most SMEs should be able to fit theirs onto a single sheet of paper. The most important thing is clarity."[53]

Most governments in Europe have issued some sort of security guidance books, based on international standards (for instance ISO or NIST), and offer a variety of support. There is no shortage of information or opportunities to obtain advice, whoever wants to receive it can find it. It looks like an incentive problem. The EU could bring ideas to the Member States on how to make the development of cyber security plans more attractive for companies. Could business organisations such as chambers of commerce not play a bigger role, maybe supported by the forthcoming Digital Europe programme?

Mandating or promoting certification has traditionally played a key role in cyber security policy, including when it comes to public procurement of ICT equipment and services. There is a wide spectrum of international security certification (e.g. common criteria, ISO certification), private security initiatives (e.g. cloud security alliance), European schemes (e.g. SOG-IS Mutual Recognition, ETSI Standards) and national frameworks (e.g. Trusted Cloud (Germany), Certification Sécuritaire de Premier Niveau (France)) to choose from. The EU has established a voluntary Europe-wide certification framework facilitating mutual recognition and building on ENISA's competence. How to make it work as part of the existing proliferation of security and trust schemes will determine its success. Certification and related 'audits' should have a value, a meaning in a regulatory sense, as they are complex and costly. Support should be given to smaller companies so they can also benefit from those schemes.[54]

Cyber security policy needs **international cooperation** and global companies to be effective. Cyber-attacks are criminal activities which cross borders. Countries must work together. Actions against global botnets for instance require international cooperation. The 'Convention on Cybercrime (Budapest Convention)' of the Council of Europe of 23 November 2001 is presumably the most comprehensive and influential framework in this regard.[55]

This approach could be taken further and expanded, for instance with a view to actions at G20 level:

"Furthermore, we recognize the growing importance of promoting security in the digital economy and of addressing security gaps and vulnerabilities. .... Along with the rapid expansion of emerging technologies including the Internet of Things (IoT), the value of an ongoing discussion on security in the digital economy is growing."

G20 Osaka Leaders' Declaration

OUTLOOK

Europe has the legal framework and financial support systems for stepping up cyber security measures in place. It needs to make sure that all these measures and regulations are implemented in a consistent way, as there is a tendency towards multiplication of efforts and complex regulations, for instance with regard to certifications.

The institutional framework could be enhanced to take into account cybercrime, for instance by reinforcing cooperation of computer security bodies with Europol and by increasing international cooperation, for instance in the context of the G20.

Policy-makers should establish tighter cooperation with industry. It is time for the industry to write more parts of the script. Policy should help.

Conclusions

CONCLUSIONS

We would like to conclude this report with three considerations.

First, throughout this paper we have stressed the importance of implementation, i.e. giving guidance on how to comply with regulation, translating principles into rules, getting investments done. The forthcoming digital policy, whatever its shape, should put emphasis on an elaborated **execution agenda**, measuring progress and impact on the ground.

Second, there is a paradox. Europe has entrepreneurs, talents and promising start-ups. Europe has first-class research and frequently leads in technology. At the same time, the **mindset** is time and again characterised by technology scepticism. Risks are highlighted, opportunities come second. Effectively changing this mindset should become a priority.

Third, leveraging **digital investments** should become a focus point. Whilst the EU budget is limited it can function as a trigger, cover some cross-border investments and support innovation. Private and public investments at a much bigger scale are needed.

Increasing the level of private investments requires a regulatory environment and a policy climate that makes it attractive to invest. This includes investments from global companies.

Public investments in digital infrastructure and also in complementary assets are necessary, as shown in the cases of rural broadband, education reforms and smart cities, and must come predominantly from Member States. This involves setting priorities, which is understandably hard. Yet, the stakes are high, and without investments at a sufficient scale, Europe will not reap the full benefits of digital transformation.

All three generic policy elements, i.e. implementation, mindset and investments, must be considered together by EU policy-makers and supported by the Member States, as they reinforce each other.

[1] http://www.standupeconomist.com/pdf/misc/solow-computer-productivity.pdf

[2] http://www.oecd.org/economy/outlook/digitalisation-and-productivity-complementarities

[3] OECD (2019), *OECD Compendium of Productivity Indicators 2019*, OECD Publishing, Paris, https://doi.org/10.1787/b2774f97-en

[4] https://www.mckinsey.com/featured-insights/regions-in-focus/solving-the-productivity-puzzle

[5] http://www.lse.ac.uk/business-and-consultancy/consulting/consulting-reports/the-evolving-role-of-ict-in-the-economy

[6] https://ec.europa.eu/info/sites/info/files/2019-european-semester-country-specific-recommendations-commission-recommendations-communication_en.pdf

[7] Global e-Sustainability Initiative (GeSI): #SMARTer2030, ICT Solutions for 21st Century Challenges, 2015 (study prepared by Accenture Strategy) http://smarter2030.gesi.org/downloads/Full_report.pdf

[8] Shift Project, Paris based think tank on energy transition. Report 'Lean ICT – Towards Digital Sobriety', published in March 2019 https://theshiftproject.org/wp-content/uploads/2019/03/Lean-ICT-Report_The-Shift-Project_2019.pdf

[9] European Commission: Final Report of the High-Level Panel of the European Decarbonisation Pathways Initiative, November 2018 https://publications.europa.eu/en/publication-detail/-/publication/226dea40-04d3-11e9-adde-01aa75ed71a1

[10] David Rolnick et al.: Tackling Climate Change with Machine Learning, 10 June 2019 https://arxiv.org/abs/1906.05433

[11] https://ec.europa.eu/digital-single-market/en/digital-scoreboard

[12] https://codeweek.eu/

[13] http://publications.jrc.ec.europa.eu/repository/bitstream/JRC106281/web-digcomp2.1pdf_(online).pdf
http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110624/dc_guide_may18.pdf
https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/european-framework-digital-competence-educators-digcompedu

[14] https://ec.europa.eu/digital-single-market/en/news/attitudes-towards-impact-digitisation-and-automation-daily-life

[15] https://www.dailyrepublic.com/all-dr-news/wires/business/rise-of-the-machines-automation-reshapes-job-market/comment-page-1/

[16] For a survey about the impact of digital transformation and in particular AI on the EU labour market, see the following two reports:
https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-impact-digital-transformation-eu-labour-markets
https://ec.europa.eu/epsc/sites/epsc/files/ai-report_online-version.pdf

[17] https://www.weforum.org/reports/the-future-of-jobs-report-2018
https://www.weforum.org/agenda/2018/09/what-if-ai-is-coming-for-jobs-faster-than-we-thought

[18] https://www.weforum.org/agenda/2019/03/the-digital-skills-gap-is-widening-fast-heres-how-to-bridge-it/

[19] https://www.capgemini.com/nl-nl/wp-content/uploads/sites/7/2015/12/digital-organisational-frameworks-and-it-professionalism.pdf

[20] https://euobserver.com/digital/137835

[21] https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_specialists_in_employment

[22] https://ec.europa.eu/digital-single-market/en/policies/improving-connectivity-and-access

[23] http://publications.europa.eu/webpub/eca/special-reports/broadband-12-2018/en/

[24] https://ec.europa.eu/digital-single-market/en/news/5g-deployment-could-bring-millions-jobs-and-billions-euros-benefits-study-finds

[25] https://www.icnirp.org/

[26] https://www.gsma.com/publicpolicy/consumer-affairs/emf-and-health/emf-policy

[27] https://www.3gpp.org/news-events/1975-sec_5g

[28] https://www.huawei.eu/file-download/download/public/1442

[29] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks

[30] https://www.mobileworldlive.com/featured-content/top-three/tim-ctio-urges-action-on-troubled-italian-market/

[31] Jean-Luc Lemmens, Soichi Nakajima, Digital Europe still in the race, in DigiWorld Watch Series (IDATE), 25 January 2018.

[32] Dr H. Gruber, Investment policy in Digital Infrastructure, EIB at IDATE DigiWorld Seminar, Dec 14 2018.

[33] https://smartcities-infosystem.eu/

[34] https://www.mckinsey.com/~/media/mckinsey/industries/capital%20projects%20and%20infrastructure/our%20insights/smart%20cities%20digital%20solutions%20for%20a%20more%20livable%20future/mgi-smart-cities-full-report.ashx

[35] http://www.eurocities.eu/eurocities/home

http://nws.eurocities.eu/MediaShell/media/EUROCITIES_-_city_leaders_agenda_for_Europe_-_March_2019-A4.pdf

[36] https://www.smartcitiesworld.net/opinions/the-three-biggest-challenges-to-building-a-commutable-smart-city

[37] The industry supporting C-V2X technology for connected cars is represented by the 5GAA: http://5gaa.org/. DSRC support is driven by the Car 2 Car Communication Consortium: https://www.car-2-car.org

[38] http://europa.eu/rapid/press-release_MEMO-17-675_en.htm

[39] https://ec.europa.eu/transport/modes/road/news/2018-05-17-europe-on-the-move-3_en

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0283&from=EN

https://eur-lex.europa.eu/resource.html?uri=cellar:0e8b694e-59b5-11e8-ab41-01aa75ed71a1.0003.02/DOC_1&format=PDF

[40] Tsinghua University's '2018 China Artificial Intelligence Development Report' http://www.sppm.tsinghua.edu.cn/eWebEditor/UploadFile/China_AI_development_report_2018.pdf

World Intellectual Property Organization (WIPO), Technology Trends 2019, Artificial Intelligence https://www.wipo.int/publications/en/details.jsp?id=4386

https://www.cbinsights.com/research/china-artificial-intelligence-investment-startups-tech/

https://www.bloomberg.com/news/articles/2019-01-08/vcs-plowed-a-record-9-3-billion-into-ai-startups-last-year

www.oecd.org/going-digital/ai/private-equity-investment-in-artificial-intelligence.pdf

[41] https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence

[42] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[43] http://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm

[44] https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf

[45] https://www.weforum.org/agenda/2019/04/dont-be-scared-of-ai-its-going-to-change-humanity-for-the-better/

http://www3.weforum.org/docs/Harnessing_Artificial_Intelligence_for_the_Earth_report_2018.pdf

[46] See also the analysis on AI for People in the following publication:

https://link.springer.com/article/10.1007/s11023-018-9482-5

[47] https://www.oecd.org/going-digital/ai/principles/

[48] https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf

[49] https://www.sentinelone.com/blog/history-of-cyber-security/

[50] https://www.comtact.co.uk/blog/endpoint-protection-epp-vs-edr-whats-the-difference

[51] https://www.mobileworldlive.com/m360-security-for-5g-news/ai-flagged-as-double-edged-security-sword/

[52] https://ecs-org.eu/cppp

[53] https://www.bsigroup.com/en-GB/Cyber-Security/Creating-cyber-security-policies/

[54] https://www.sogis.eu/

[55] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561


HUAWEI