OLIVER WYMAN

EUROPEAN DIGITAL SOVEREIGNTY

Syncing values and value

Emmanuel Amiot
Ivan Palencia
Augusto Baena
Charles de Pommerol

CONTENTS

EXECUTIVE SUMMARY

The digital economy is expected to add 1.1 percentage points to the European Union's annual economic growth and to boost GDP by over 14 percent by 2030.[1] That implies an extra €2 trillion of GDP by 2030, which is similar to Italy's current GDP.

Today, however, Europe relies on overseas companies for most of its digital life. The digital identity of many European citizens depends on foreign email addresses; 92 percent of the western world's data is stored in the US.

This digital dependence is a major problem. To thrive economically, Europe needs to become a leading digital economy, but this will only be possible if Europe regains control, trust, and sovereignty in data and digital technology. We think Europe will only be able to transform itself into a digital leader if it can deliver a digital action plan combining four basic elements.

1. **Connectivity and 5G.** The cornerstone of the digital economy is boundless, high-speed, secure connectivity. Yet declining revenues meant that European telecom operators' return on capital employed fell by 5 percentage points between 2013 and 2018, making Europe an increasingly unattractive market to invest in relative to its peers in the US and China. The net effect was that there 40 percent less available investment capital per capita for telecoms networks, compared to the US over the past decade. A major reason is the fragmentation of its market.
2. **Computing infrastructure.** Data will progressively move to local storage, such as mobile devices or connected vehicles. That makes it critical to implement a distributed cloud and edge infrastructure built on upon Europe's mobile networks.
3. **Data and artificial intelligence.** For citizens and organisations to have data sovereignty, they should have reasonable and efficient access to an end-toend data journey integrating three elements:
   - Gigantic, high-quality datasets with fair rules for access and use
   - Algorithms and computational resources for ready-to-deploy solutions
   - Secure storage of data governed by European laws

   Without efficient access to huge amounts of harmonised data and computing infrastructure, it will be impossible to develop a leading-edge artificial intelligence sector. Europe also needs a higher level of skills and innovation: It invests half as much as China and only one-fifth as much as the US in tech research and development, though Europe and US have similar GDPs and China's economy is 30 percent smaller.[2]
4. **Cybersecurity.** Within five years, a 5G-network outage could have an impact comparable to that of an electric power cut today. But Europe suffers from a growing cyber-skills shortage due to a misalignment between formal education and private-sector demands. Future cyber-defence will increasingly depend on the exploitation of data with advanced AI and the leveraging of 5G architecture.

1 European Commission.

2 EU Commission R&D Scoreboard — US, China, and EU values include America, APAC, and EMEA companies, respectively.

In short, Europe today does not have access to the four elements required to thrive in the digital economy. One result is that Europeans are largely dependent on foreign digital technology companies. In 2019, the market capitalisation of the four biggest US and four biggest Chinese tech companies was 17 times the market capitalisation of the top 10 EU telcos.

There are four important ways in which Europe can begin to recover digital sovereignty and form a basis for its digital economy to grow.

1. **Join forces to build 5G infrastructure.** First, costs should be spread, and investments should be targeted at areas that are likely to boost industrial competitiveness. For 5G, that means operators together building an interoperable European open radio access network (O-RAN) — a new way of building RANs, based on software infrastructure. Operators should be able to form focused alliances with industries in which Europe leads, such as the automotive, healthcare, and energy sectors. Bigger, well invested shared networks allow mobile operators to compete on services whilst pooling resources in infrastructure, avoiding duplication of effort. These groupings could trigger the development of clusters of laboratories around Europe that form islands of technology innovation. Governments and the EU could allow tax breaks and let telecom companies issue “digital bonds” under favourable conditions. They should take into account the benefits of such groupings in the development of new products and services and amend competition policy accordingly. And specific 5G regulations should be designed to guarantee that transmitted data is secured and regulated in Europe.
2. **Build a European distributed cloud and edge infrastructure.** A second essential component of the digital future is the development of new services based on a distributed cloud and edge infrastructure largely available, and based on European rules on topics such as data storage and processing. Strengthening and accelerating European secured and distributed cloud, such as Gaia-X, the Franco-German initiative, is essential. This would enable data infrastructure and services that comply with strict data protections rules. Allowing Europe to form a wide coalition of industrial companies which offer a broad range of digital services.
3. **Develop an industrial data strategy.** A third pillar is an industrial strategy for data. This needs a new legal and regulatory framework. One condition is regulation that protects data as property, just as a house is protected. Also needed is a standard, EU-wide definition of sensitive data and the rules governing the storage and processing of this data. The General Data Protection Regulation (GDPR) was a step forward for individuals; similar rules and principles are now needed for data used in business-to-business interactions. In addition, pan-European data alliances that enforce data portability rights can create new arenas for data and distributed AI at the edge. Then, data will be increasingly stored in Europe, and both individuals and organisations should be able to obtain secured European sovereign digital identities. Further, European education must also evolve to give greater importance to digital skills, such as artificial intelligence and cybersecurity.
4. **Develop a European cyber leader.** Fourthly, Europe needs leading-edge cyber technology. A first step is links between the defence and private sectors, which could mobilise defence budgets and build cyber products for both military and civilian use. European companies should be encouraged to form alliances so as to mutualise assets and share data. Some of this could be made systematic potentially through a central organisation such as CERT-EU, the computer emergency response team for the EU institutions and agencies. Europe should also create a leading cybersecurity campus, as well as European cyberproof labels to raise awareness of cybersecurity and encourage the development of capabilities.

Achieving digital sovereignty and increasing the scale of Europe's digital industry will be costly — probably more than €500 billion, according to our calculations: €130 billion for 5G; €200 billion to build a distributed cloud and edge infrastructure; €100 billion to boost artificial intelligence; and €100 billion to improve cybersecurity defences. The funds will have to come from both public and private sources. If spent judiciously, they could propel Europe's digital economy forward much faster than is currently projected. These investments will lead to the creation of high valueadded jobs and can help shorten the gap in digital skills while feeding a virtuous circle.

5G represents a technological turning point, and Europe has a chance to change the structure of the digital world and achieve digital sovereignty. Success will need rapid, large-scale action — and, while investing more will be important, it will not be sufficient. To succeed, the EU must develop a path aligned with its values of cooperation and security and rely on its digital assets, the most notable being telecom operators.

HUGE DATA GROWTH HIGHLIGHTS THE IMPORTANCE OF SOVEREIGNTY

DIGITAL ECONOMY TO ADD 14 PERCENT TO EU GDP BY 2030

The digital economy is expected to add 1.1 percentage points annually to the European Union's economic growth and to boost GDP by more than 14 percent by 2030.[3] That implies an extra €2 trillion of GDP by 2030, which is similar to Italy's current GDP.

One key element in the digital economy's contribution to growth is data. The quantity of global data processed is expected to increase from around 50 zettabytes — that is, 50 trillion gigabytes — to 175 zettabytes by 2025, implying a compound annual growth rate of 27 percent. This huge growth will be enabled by 5G networks and the Internet of Things (IoT).

Data is a strategic point of control and the basis for companies to excel in personalised customer experience, enabling them to maintain close relationships with their customers and bypass middlemen. It is also a powerful lever to achieve operational efficiency and to create innovative value propositions, both of which can lead to a better use of resources and help achieve the EU's Green Deal to become carbon neutral by 2050. For example, it has been estimated that 5G-enabled smart grids have the potential to reduce household gas consumption by 12 percent.[4] European operators can be key partners in taking advantage of 5G's new functionalities to bring digital innovation to industrial sectors such as automotive, manufacturing, and agriculture.

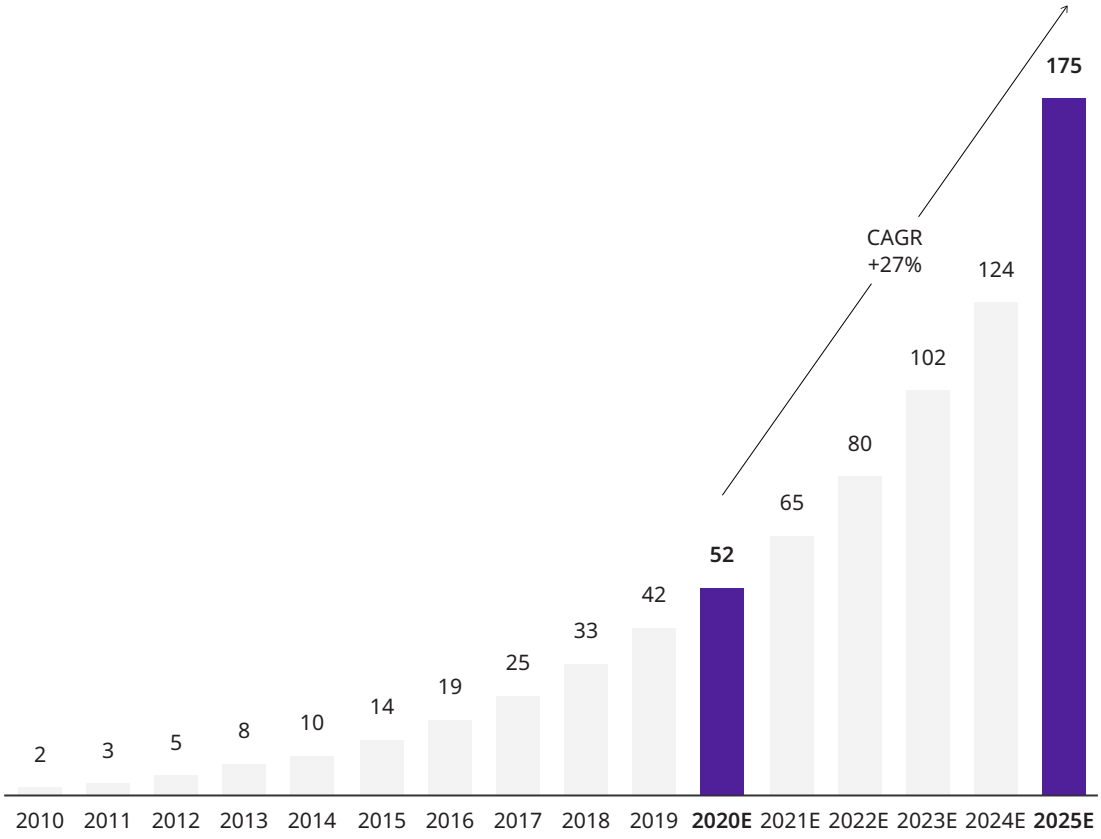
3 European Commission.

4 O2.

Data growth goes hand-in-hand with the creation of jobs, some of which will be very well paid. Currently, Europe is short about 500,000 data scientists and analytics experts, a gap that is expected to double by 2025.[5]

The value of the EU data economy — considering the direct, indirect, and induced impacts of the exploitation[6] of data — will double by 2025, according to IDC. In 2018, the EU data economy represented 2.4 percent of GDP (€380 billion), and it is expected to reach between 4.2 percent and 6.3 percent by 2025. The value generation will not only come from traditionally data-intensive companies and sectors. Data is being increasingly used in industries such as mining and manufacturing to automate operations and create new products and services.

Exhibit 1: Global digital information created per annum
In zettabytes

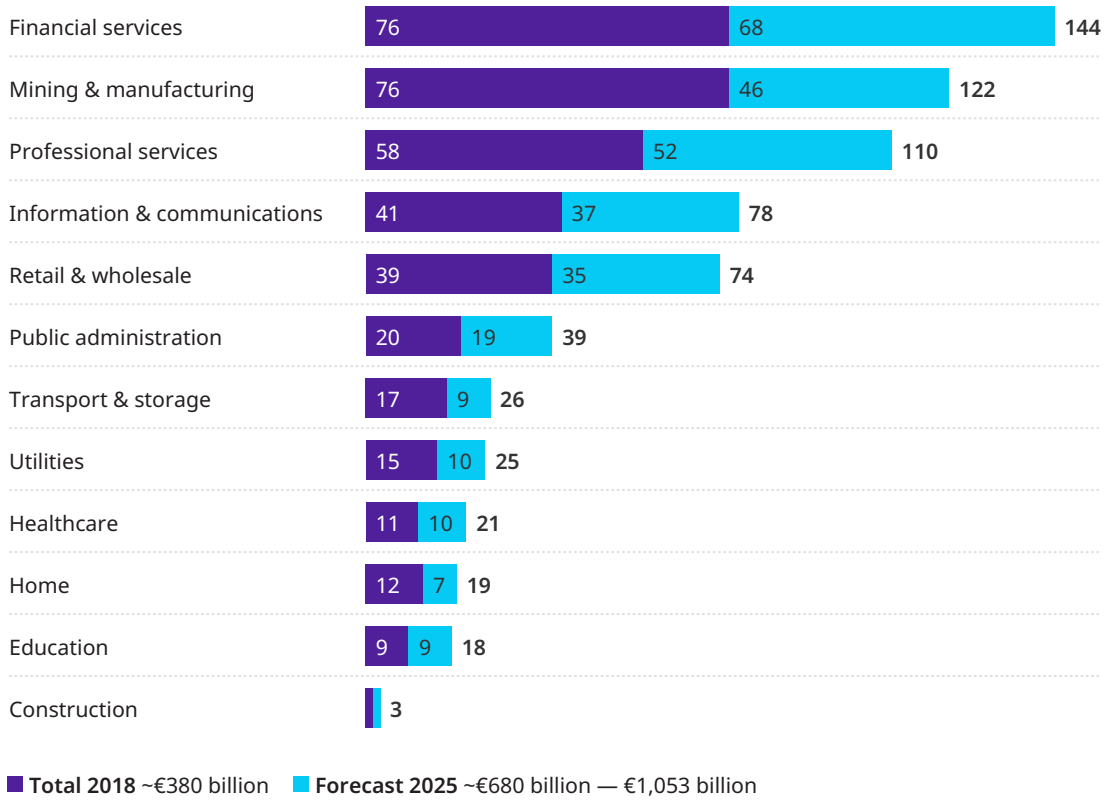


Source: IDC Data Age 2025 report, Oliver Wyman analysis

5 IDC: European Data Market Update Smart 2016/0063.

6 Includes the generation, collection, storage, processing, distribution, analysis elaboration, delivery, and exploitation of data enabled by digital technologies.

Exhibit 2: Total impact of the data economy per industry in the European Union
2018-2025 in € billion



Source: IDC — European Data Market Update Smart 2016/0063

NEW USES, NEW ECOSYSTEMS

Use case #1
Highways for autonomous driving

China has been promoting 5G-enabled self-driving vehicles in an attempt to lead the world in autonomousdriving innovation. In 2019, a $150 million investment aimed to build 2,000 5G base stations in Wuhan for testing use cases including autonomous driving.

Three Chinese companies were granted licenses to operate commercial transport services with self-driving vehicles, which are expected primarily to be buses. The vehicles will be allowed to provide services on 28 kilometres of public roads in Wuhan. It is hoped that the use of 5G and a Chinese satellite will reduce latency to just a few thousandths of a second and enable centimetre-level positioning accuracy. Wuhan has extended the new services to 159 kilometres of public roads, covering 90 square kilometres. In other parts of China, additional 5G-enabled technologies are being deployed and tested, such as C-V2X, which supports communications between vehicles and infrastructure, such as smart toll stations.

Use case #2

Remote surgery

Many patients requiring specialist surgery cannot afford to travel to the necessary healthcare professionals, particularly in cases where they have rare conditions that only a few surgeons in the world can treat. Using 5G mobile networks, a surgeon in a remote location could react to physical and visual stimuli in less than 10 milliseconds. Until now, it has taken much longer than this to compress and decompress video content and tactile feedback for long-distance transmission, so remote surgery has been impossible.

When operating via a robotic intermediary over a 5G network, surgeons can use specialised haptic feedback gloves. The gloves give a surgeon the same sense of touch as if they were standing over the patient, while video from the operating theatre is streamed in real time. The world's first remote operation using 5G technology was carried out in China in 2019, when a doctor controlled robotic arms 50 kilometres away to remove the liver of a laboratory test animal. Two months later, a doctor inserted a stimulation device into the brain of a Parkinson's patient nearly 3,000 kilometres away.

Use case #3

Passenger and freight drones

Most large cities suffer from traffic congestion. To get around the problem, a German company has created vertical take-off drones that could transport both people and goods. The first use case is expected to be air taxis connecting airports to city centres. Intracity, and then intercity, routes could follow.

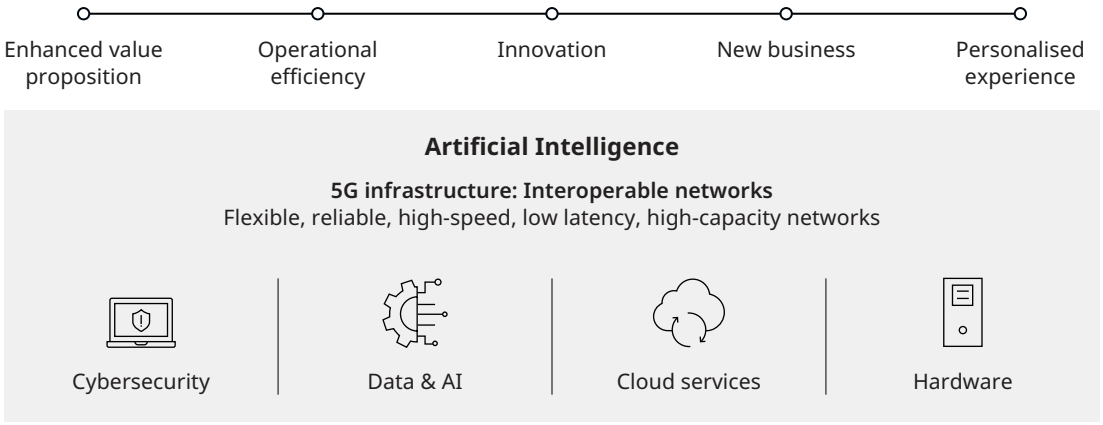
The company is now integrating 5G technology to enable its drones to fly farther and more safely. The rapid flow of large amounts of data will help provide richer information on the drone's surroundings and enable the download of flight data to enhance performance and safety. In addition, 5G is expected to allow VoloDrone, an autonomous freight version, to carry out tasks such as crop spraying, surveying, and the delivery of bulky items.

Use case #4

Smart port

In 2019, one of the largest Chinese ports demonstrated an automated ship-to-shore crane for containers that is operated from a control centre over a 5G connection. The connection facilitated data traffic from more than 30 high-definition cameras, as well as control data that was processed by a programmable logic controller. The operation was made possible by 5G network functional drivers, which included millisecond-level latency control signals and offered stable, remote real-time control. The trial showed that a port that is fully automated using 5G functionalities could reduce labour costs by 70 percent.

Exhibit 3: The core elements of the data economy



Source: Oliver Wyman analysis

WHY DIGITAL SOVEREIGNTY MATTERS FOR EUROPE

The basis for these applications and other future value propositions is 5G connectivity, which will facilitate high-speed data transfer with very low latency. Billions of devices will be interconnected with unprecedented processing power and storage capacity, making available vast amounts of data. But this data will only be useful in the context of end-to-end data journeys. These depend on the core elements of digital interaction, such as 5G networks, cloud and edge devices, cybersecurity, and artificial intelligence.

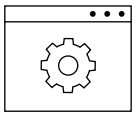
Why are these so important? At present, Europe depends on non-European services and enablers for most of its digital activities. The digital identity of many European citizens depends on US email addresses of the form @xxx.com, and 92 percent of the western world's data is stored in the US.[7] As the volume of data grows, companies and citizens could become increasingly "locked-in," as it becomes harder to move their data to other platforms.

Recent legislation gives the US government access in some circumstances to data stored by US technology companies, independent of where the data are physically stored. So, while European companies and citizens become more dependent on data, they are also becoming more dependent on foreign countries. This is one reason that European Commission President Ursula von der Leyen has made technology sovereignty a priority.

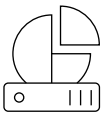
European digital sovereignty will empower citizens and companies to decide which data can be gathered, shared, used, and saved. There are three conditions for data sovereignty: 1) quality datasets with fair rules for access and use; 2) secure storage; and 3) algorithms and computational resources for ready-to-deploy solutions. If one of the three is missing, the whole chain is jeopardised.

7 Atlantic Council: Waving the flag of digital sovereignty.

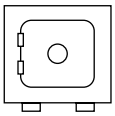
Exhibit 4: European data sovereignty



Algorithms and computational resources
For ready-to-deploy solutions



Huge and quality datasets
With fair rules for access and use



Secure storage
Governed by European laws

Source: Oliver Wyman analysis

THE NEXT DIGITAL WAVE: EUROPE, THE US AND CHINA

DIGITAL INVESTMENT AND SKILLS

Europe is a major player in the world economy, generating about a quarter of global output[8], as measured by GDP. Europe is also home to some of the world's most important industrial enterprises, including major vendors of 5G equipment, large automotive companies, and leading telecom players. However, Europe is lagging the United States and China in digital technology.

One reason is that European companies do not invest as much as their foreign rivals. European enterprises on the list of the world's 500-largest tech companies invested a total of €27 billion in tech research and development in 2018. That was half as much as the Chinese companies on the list, which invested €50 billion; and one-fifth of the amount invested by US companies on the list — €134 billion.[9] (Europe and the US have similar GDPs, while China's is about 70 percent the size.) Overall, the top four US tech companies and the top four Chinese tech firms invested over €270 billion in R&D from 2014 to 2018.[10]

European venture capital investments were about a fifth of those of the US and China relative to GDP in 2018.[11] These lower investments in tech innovation have resulted in a lag in cloud infrastructure and hardware manufacturing. Similar gaps are observed in privateequity investments in artificial intelligence: Worldwide, about 80 percent are in US and Chinese companies, and just 8 percent in European.[12] At the same time, both the US and China are investing substantial public funds in AI. The US budget for 2020 alone, for example, was close to €2 billion, including spending by the Department of Defense. The European Union is planning to invest a mere €2.5 billion in AI from 2021 to 2027 — though that figure is just for EU funds and does not include funds from member-state governments.

8 World Bank: GDP values in 2018 — European Union ~$18.78 trillion and Global ~$85.91 trillion.

9 European Commission: "The 2019 EU Industrial R&D Investment Scoreboard".

10 Capital IQ: GAFA and BATX R&D investments 2014 to 2018.

11 Forbes: "Raising Venture Funding In Europe vs. the US".

12 Organisation for Economic Co-operation and Development: "Private Equity Investment in Artificial Intelligence".

Exhibit 5: Digital capabilities scorecard

US, China, and the European Union

Source: Oliver Wyman analysis

Around 80 percent[13] of data in the cloud is stored by five large tech companies, none of which is European. In hardware, no European company was among the top 10 providers of semiconductors by sales in 2019.[14] The EU is also behind in the number of producers of AI chips, with 12 firms; China has 36 and the US 55.[15]

Moreover, Europe is lagging in digital talent. The shortage of digital and data skills is a global problem, driven by an ageing population among other factors: In member countries of the Organisation of Economic Cooperation and Development, 56 percent of adults have no — or only very basic — skills in information and communications technology.[16] However, China and India have produced fast-growing numbers of STEM (science, technology, engineering, and

13 Gartner, July 2019.

14 Intel: Intel to Reclaim No.1 Semiconductor Supplier Ranking in 2019.

15 Abacus: "China's AI firms need alternative hardware", October 2019.

16 Organisation for economic co-operation and development: Skills Outlook.

mathematics) graduates. The two countries could account for more than 60 percent of the STEM graduates in major economies by 2030, compared with only 8 percent for Europe and 4 percent for the United States.[17]

Europe has recently accelerated its fibre deployment, but it is behind the US and China in 5G. The four main US telcos have already launched 5G commercial services in more than 40 cities[18], and commercial services are available in more than 50 cities in China.[19] However, while Europe aims to deploy 5G in all major urban areas and along major railways by 2025, so far only nine EU countries[20] have launched commercial 5G services, and Europe has only about 3,000 base stations.[21] China has already deployed 130,000 5G[22] base stations and the US 10,000.[23] Today, China has 94 5G stations per million inhabitants; the US 31; and Europe just seven.[24]

Exhibit 6: Current situation

In 2019

Digital giants domination
Top four US and Chinese tech companies market cap equivalent to

17x

the market cap of the top 10 European telcos

Tech R&D investments
European tech companies invest

2-5x

less on R&D than China and US

Cyber resources

60%

of European SMEs have insufficient resources for cyber defence

By 2030

Data storage

92%

of the western world's data is stored in the US

Network investments
European telcos have invested

40%

less than what the US have done over the past 10 years

Digital skills

8%

of STEM graduates from Europe vs. 60% from China and India

Source: Oliver Wyman analysis

17 BBC: China opens a new university every week.

18 Digital trends: Here are the cities where you can access 5G from major US carriers right now, January 2020.

19 CNN article: China just launched the world's largest 5G network, November 2019.

20 Excluding the United Kingdom.

21 IDATE: "5G Observatory quarterly report 6" and Oliver Wyman analysis.

22 The Telegraph: "China will have 130,000 5G base stations by the end of year".

23 IDATE: "5G Observatory quarterly report 6".

24 World Bank, The Telegraph, Wall Street Journal, European Commission Observatory report, Oliver Wyman analysis.

China's quick deployment is thanks partly to its capacity to effect changes that speed up the process. Policymakers have modified the regulatory framework, allowing state-owned companies to receive privatesector funding to improve decision-making and competitiveness. To spread the cost of investment, two of the largest players have set up a co-build co-share cooperative framework where one player will build 60 percent of the network and the other the remaining 40 percent.

THE SCALE OF THE DIGITAL GIANTS

The tech giants are becoming increasingly dominant and capturing a disproportionate share of the digital ecosystem. The winner-takes-all nature of many digital products has led to a new class of oligopoly named after the market capitalisation its members have achieved: "the $1 trillion club." The market capitalisatio of the global tech giants in 2019 was nearly €5.2 trillion, 17 times the market capitalisation of the top 10 European telcos.[25]

This asymmetry is having an impact on the development of the European data economy. The overseas giants' massive cash reserves allow them to invest in promising bright ideas: In total, they have acquired about 1,000 companies since 2010. Coupled with their strong R&D investment, this intense M&A activity is helping the tech companies to widen the gap with Europe.

THE COMING OPPORTUNITIES: FROM 5G TO AI

Europe faces major challenges as it tries to deploy digital infrastructure, simplify access to data, and strengthen cybersecurity and artificial intelligence.

BOUNDLESS, HIGH-SPEED, SECURE CONNECTIVITY

There is a clear correlation between the level of investment in telecommunication networks and an economy's degree of digitisation. The US and Canada, for example, invested about twice as much per capita as France and Germany in their fixed and mobile networks between 2008 and 2018, fueling higher data consumption and a greater degree of digitisation.[26]

25 Capital IQ.

26 Ovum, WCIS, WBIS, World Bank, Oliver Wyman analysis.

Overall, Europe has invested 40 percent less per capita in its telecoms networks than the US over the past decade. A major reason is the fragmentation of its market. Ninety European operators serve 445 million inhabitants[27], while in the US four operators serve 320 million inhabitants.[28] As a result, the European sector has been losing appeal for investors, which, in turn, short-circuits the capacity of the sector to invest in the much needed telecom infrastructure to close the gap. Europe's fragmentation has led to two distinct problems: excessive capital intensity, with consequent high debt burdens; and intense retail price competition, which limits the sector's ability to improve its return on capital. Despite their relatively low investment levels, European telecom operators' return on capital employed fell by 5 percentage points between 2013 and 2018.[29] As a result, the European sector has been losing appeal for investors.

STRONGER ARTIFICIAL INTELLIGENCE CAPABILITIES

Data has become a new asset class. Gigantic data is needed to train AI systems so that they reach increasing levels of skill, starting with pattern recognition and moving onto more sophisticated prediction techniques. The more data that can be accessed, the smarter the algorithms can become. And the smarter the algorithms, the better the services they will help to provide — and the more people will bring their data to be worked on. Data and AI thus create a virtuous circle.

But data will only become available in sufficient quantities under the right conditions. One of these is a reduction in fragmentation. Currently, there are multiple flaws in Europe's data environment. There are limited data interoperability standards, and there are no tools or infrastructure to support the creation of data pools with rich sets of structured data, of the kind that could facilitate big-data analytics and machine learning. Moreover, while the GDPR sets conditions for the use of individuals' data, there is no regulation governing the access and use of data between businesses. In 2025, 60 percent of data will come from industry, and it will play a vital role in the future of sectors ranging from manufacturing to healthcare.[30] So Europe needs a trusted environment for data, both consumer and industrial, which could involve various kinds of regulatory action. It is not clear whether the antitrust remedies that worked for telecoms would be effective for regulating the software-based networks that dominate the digital era, but that option should be considered. Without establishing a framework to make data available in the right conditions, Europe will not be able to develop effective AI capabilities.

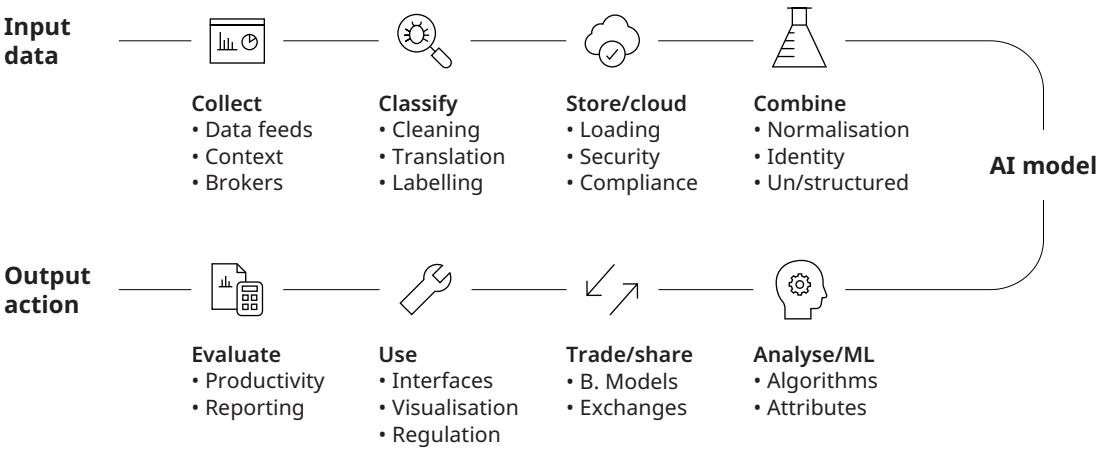
27 Excluding United Kingdom.

28 AT&T, Verizon, T-Mobile, and Sprint capture 96% of the market share in terms of mobile subscription.

29 Mobilise: "Telecommunications, is it a declining business model?".

30 IDC.

Exhibit 7: End-to-end data journey



Source: GSMA Intelligence

CYBERSECURITY

Why it matters more than ever

Cybercrime is estimated to be the most frequent illegal activity in the world, and it will continue to present a major challenge.[31] About 1.2 billion people in 16 countries have been the victim of a cybercrime, according to the 2018 Norton LifeLock Cyber Safety Insights Report. The total financial cost of cybercrime in 2019 was more than $1 trillion, according to the Marsh & McLennan Cyber Handbook 2019. Cyber risk adds significant uncertainty to national economies and corporate business models, and within five years, a potential 5G network outage could have an impact comparable to that of an electric power blackout today.

The variety of cyber risks is increasing. Data-rich capabilities, tools, and apps offer a larger attack surface and greater consequent exposure to cyberattacks. Demand for integrated consumer solutions means a decrease in checks and authentication gateways, so products, devices, businesses, and individuals are increasingly connected, giving attackers a greater number of entry points. This interdependency of devices — "digital seamlessness" — means the point of intrusion is not necessarily the ultimate target.

Connectivity and integration mean that risks tend to become systemic, making them harder to manage and control — and harder to quantify and visualise. Risk-management tools and cyber-testing protocols provide some reassurance, but most organisations and individuals are not able to estimate the cost of losing control of their data.

Other challenges come from advances in areas such as AI that increase cyber risk by encouraging greater collection and sharing of data or by making it easier to cause damage and carry out manipulation and fraud. Most cyberattacks could not have been predicted from previous attacks.

31 Centre for Strategic and International Studies (CSIS).

Amid these growing risks, Europe faces a shortage in its workforce's cyber skills, resulting from a misalignment between formal education and private-sector requirements and from a lack of nonformal training opportunities. The number of unfilled cybersecurity jobs has grown by more than 50 percent since 2015[32], and today around 60 percent of small and medium businesses lack the skills[33] to ward off cyber threats. As a result, many IT systems are insecure; corporations have limited ability to assess their cybersecurity; and there is a skills gap between attackers and defenders. The problem will likely become more severe in the near term.

AI and machine learning have the potential to prevent, detect, and respond to cyberattacks. And 5G is potentially more secure than 4G, as its 256-bit encryption can cover more data. But humans are the weakest link. Around 80 percent of data breaches are associated with the interface between humans and technology — such as when sensitive documents are sent to unintended recipients, a member of staff falls for a phishing attack, or unauthorized users access corporate devices. Password practices are another common risk.

Unfortunately, these risks do not decrease with more stringent protocols, as employees tend to become noncompliant, especially in organisations that view cybersecurity only as an IT problem. Attempts to eliminate human error can shift the risk to centralised system vulnerabilities, which increase the potential impact of an attack. The growing cyber threats have led to a divide in resilience. Large corporations have the human and technological resources to invest in cyber resilience, whereas small and medium businesses do not. The lack of preparedness at small and medium enterprises (SMEs) leaves large parts of Europe's digital economy exposed. Two out of three SMEs have been attacked in the past year; 60 percent have insufficient resources for cyber defence; and 40 percent have no incident response plan, according to a recent UK survey.

TIME TO BUILD EUROPEAN CLOUD AND EDGE INFRASTRUCTURES

Europe's lack of its own cloud infrastructure is a potential threat to privacy and security. European companies and governments store much of their data with foreign-based firms.

The adoption of 5G will lead to a fundamental shift in data storage. Today, 80 percent of data is stored in the cloud and data centers. But this will shift to local and edge storage — that is, storage in devices such as smartphones and connected cars. In five years, local storage will account for 80 percent of storage.[34]

For Europe to become a key enabler of this new data space, it will need its own distributed cloud and edge infrastructure that will bring computing closer to the source of data — minimising the distance between the client and the server.

32 Oliver Wyman Forum: "The Seven Most Pressing Challenges Facing Cybersecurity".

33 Beaming: "The 2018 State of Cybersecurity in Small and Medium Size Businesses".

34 Les Echos: "Pour accéder au marché européen, il faudra accepter nos règles".

THE COST OF DIGITAL SOVEREIGNTY

€530 billion over five years

Digital sovereignty for Europe will come at a cost — in the region of €530 billion. This investment should be supported by politics, regulators, and industry leaders. The deployment of 5G in major urban areas and along major railways and roads in the EU will cost about €130 billion, according to an Oliver Wyman estimate.[35] Based on investments by US tech giants, we estimate that building a scaled European cloud infrastructure will cost about €200 billion.

Major improvements in AI — to make effective use of data — will need about €100 billion in investment over the next five years to match the level of investments from other region. Cybersecurity — to provide a safe data ecosystem — also needs about €100 billion over the next five years: The US government budget for cybersecurity is close to €20 billion[36]; China spent €7 billion on cybersecurity in 2019, and this is expected to grow at about 25 percent a year.[37] For the EU, €100 billion is equivalent to about a tenth of member states' combined defence budgets.

These investments will lead to the creation of high value-added jobs and can help shorten the gap in digital skills while feeding a virtuous circle.

A DIGITAL ACTION PLAN FOR EUROPE

Data is growing in value as a strategic asset, and to achieve digital sovereignty, Europe must go beyond incremental changes. It must take major steps forward that are faithful to European values, while at the same time boosting the digital economy so that it is proportion to Europe's overall economic stature. Four actions can contribute significantly to this ambition.

35 Oliver Wyman.

36 Whitehouse: Cybersecurity funding.

37 Xihuanet: China to lead global cybersecurity market growth in next five years.

Exhibit 8: Key European actions required

Joining forces to build 5G infrastructure

- Build an open, interoperable O-RAN infrastructure based on a common framework, a fair business model
- Focus on vertical industries where Europe leads, develop an island of connectivity for large-scale testing and learning
- Design fit-for-purpose 5G regulation leveraging the "5G security toolbox" to ensure that data transmitted by 5G is secured
- Support infrastructure creation by providing funding, offering tax breaks, facilitating the issuance of long-term debt, and allowing consolidation under certain conditions

Build a European cloud and edge infrastructure

- Support a pan-European project to deploy a distributed cloud and edge infrastructure, by drawing lessons from past coalitions and potentially building on Gaia-X
- Study different regulation possibilities to guarantee European data confidentiality and privacy
- Coordinate tax systems to meet the challenges of the digital economy

Develop a data industrial strategy

- Harmonise physical and digital European rights by applying the same rules to the digital world as to the physical one; enable the creation of safe "data homes"
- Harmonise regulatory frameworks by defining sensitive data and setting up rules for B2B data interactions
- Foster pan-European data alliances and use standards to enforce data portability rights
- Store data in Europe, and encourage the use of European domain names, so that everyone has a sovereign digital identity

Develop a European cyber leader

- Link European defense budgets and cybersecurity to fund cyber technologies with both military and civilian applications
- Support voluntary data sharing for cybersecurity purposes, potentially leveraging the CERT-EU
- Build a European cyber campus to attract, educate, and retain the best talent and combine cyber and AI skills
- Build European standards such as cyber-proof labels to promote European cyber capabilities and raise awareness

Source: Oliver Wyman analysis

JOIN FORCES TO BUILD 5G INFRASTRUCTURE

Build an open, interoperable O-RAN infrastructure. Operators should together build an interoperable European open radio access network (O-RAN) for 5G. The O-RAN model[38] is a new kind of RAN with an open infrastructure centred on software. Its open, interoperable framework enables devices to switch seamlessly between different networks. That means, for example, that devices used in critical systems — say, in transport or manufacturing — can continue to operate in different locations and are protected against potential network failure.

This ability makes it easier for networks to mutualise their efforts and resources. O-RAN should be operated through a fair business model that uses sharing schemes. For instance, infrastructure could be provided as a service to third parties competing on the service layer.

38 Radio Access Networks (RAN) are antennae that facilitate the connection of devices over a network. In the past they were built using vendors' proprietary technologies, which had limited interoperability.

Focus on vertical industries relevant to European competitiveness. Operators should test new standards at scale in industries where Europe is a leader. These include the transport and automotive sectors, where Europe accounts for about 25 percent of global value added (GVA); energy, where it is at 28 percent; and healthcare, also with 28 percent of GVA. Clusters of large laboratories could form islands of connectivity and innovation, where technology would be tested and scaled. Other issues, such as the impact of regulatory changes, could also be studied. Europe could consider fostering the creation of these islands by easing or lightening regulation.

Design fit-for-purpose 5G regulation. Specific regulation is needed at EU level to ensure that data transmitted by 5G is secured and regulated. A first "5G security toolbox" — set of measures for an EUcoordinated approach to secure 5G networks — exists and needs to be expanded with additional features such as data audits, which could be overseen by national telecommunications regulators.

Support infrastructure creation. Telecom operators could be allowed to issue "digital bonds" to ease the burden of long-term funding for 5G and other digital projects. Just like green bonds, which fund environmental projects, digital bonds would benefit from tax exemptions and credits. The EU could also introduce a Europe-wide tax-benefit programme to encourage investment in tech R&D; this could be similar to the CICE tax programme (Tax Credit for Employment and Competitiveness) that operated in France from 2013 to 2019. The cost burden of digital infrastructure could also be reduced through tax cuts or by using European transformation funding, such as the Digital Europe programme.

Regulators should not hinder consolidation of the fragmented telecommunications landscape. They should evolve the current frameworks that govern the general competition implementation of the EU Directorate-General for Competition in instances where consolidation would improve capital efficiency, build Europe's digital capabilities, and have no adverse impact on consumers.

BUILD A EUROPEAN CLOUD AND EDGE INFRASTRUCTURE

Support a pan-European project to build a distributed cloud and edge infrastructure. This project would provide data infrastructure and related services with European "DNA" — that is, in a way that both allows the development of new use cases and complies with Europe's strict data protection rules. One possible basis could be the Franco-German initiative Gaia-X, which has been conceived with a similar aim. Despite being at a preliminary stage, Gaia-X has received backing from more than 100 organisations and corporations.

Europe can take lessons from the success of some previous coalitions, notably Amadeus and Airbus. Amadeus — the global distribution system (GDS) that provides search, pricing, bookings and other services for travel providers and agencies — grew out of a partnership between multiple airlines. They wanted to create an alternative to the US GDS. Since its foundation in 1987, Amadeus has become one of the largest GDSs in the world, and it now has a market capitalisation of €32 billion.

Airbus was created by France, Germany, the Netherlands, and Spain. It was launched in 1970 "for the purpose of strengthening European cooperation in the field of aviation technology," and 25 years later had achieved a 50 percent share of the global market. It is now the world's largest supplier in terms of the number of planes delivered.

Implement a European Cloud Act. Europe should also study different regulation possibilities to guarantee data confidentiality and privacy in Europe.

Coordinate tax systems to meet the challenges of the digital economy. The tax systems of different EU member states should be revised to deal with the new challenges presented by the digital economy.

DEVELOP A REAL DATA INDUSTRIAL STRATEGY

Harmonise physical and digital European rights. To ensure that data is securely stored, it should be protected by similar rules to those that apply to physical property. Everyone should have the right to a "digital home" in which to store their data

At the same time, EU regulations should be unified to progress towards a digital single market and eased to make it simpler to start new tech and data-enabled businesses. In particular, the various existing regulations on data and AI should be simplified and harmonised. For example, the ePrivacy Directive should be aligned with the General Data Protection Regulation (GDPR) in a way that enables mobile network operators (MNOs) to innovate and build data-based business models that respect European values.

Harmonise regulatory frameworks. Europe should also develop a standard, EU-wide definition of what data is sensitive — such as health data, personal data in interactions with businesses, and industrial data for business-to-business interactions. It should then establish strict rules for the storage and processing of this data. In addition, Europe needs rules and principles similar to the GDPR for data used in business-to-business interactions. These would reduce switching costs and ease the problem of vendor lock-in, making it simpler for companies to transition to a European data infrastructure.

Foster pan-European data alliances. Individuals and organisations should be able to access all their data in a single personal cloud or "data home." This would also store data created by IoT devices, which would be sent directly to the data home. Under this system, different services will access the data home — rather than users accessing services in order to retrieve their data.

To make data homes possible, Europe must decide rules that favour the rise of large data ecosystems and fully actionable data portability rights. One result will be that big tech companies will need to move away from their current business model of leveraging data for advertising purposes — as they will not be able to access data stored in data homes. Additionally, a single AI-based service will be able to access gigantic volumes of data without needing to transfer it elsewhere. This convenience will encourage the development of artificial intelligence, especially distributed AI that operates in the edge.

Store data in Europe and encourage the use of European domain names. To keep European data stored in Europe, a distributed infrastructure and ecosystem of services should be set up. European companies should be encouraged to use European domain names ("xxx.eu"), and it should be made easier for all Europeans to obtain email addresses based on such domain names. This will help to give people secured, European digital identities, which can be stored by a sovereign European aggregator. The necessary infrastructure to do this securely could be built using blockchain technology.

At the same time, Europe must upskill and reskill its workforce through public-private partnerships and a mandatory digital school curriculum, where students would learn the basics of AI, cybersecurity, and blockchain. European countries should stop building concurrent initiatives and instead share resources and best practices.

DEVELOP A EUROPEAN CYBER LEADER

Link European defence budgets and cybersecurity. Linking European cybersecurity and defence could boost funding and innovation for the development of cyber technologies for use in both military and civilian areas and developing cutting-edge decentralised (zero-knowledge) security products. It could enable the creation of a European cyber leader that combines cybersecurity with AI to detect and autonomously respond to cyber threats missed by legacy systems.

Support voluntary data sharing. Private and public European companies should consider ecosystems beyond the walls of their organisations, so that they can mutualise assets and share data for cybersecurity the natural choice. Some existing organisations could form the basis for future cooperation. In the public sector, the European Computer Emergency Response Team leverages IT security experts and information across EU institutions and agencies. In the private sector, several alliances have emerged, including the Cyberthreat Alliance, the Global Cyber Alliance, and the Trusted Computing Group.

Build a European cyber-expert campus. Europe must create a leading cybersecurity campus to attract, educate, and retain the best talent by combining cyber capabilities with AI applications. Such institutions already exist at the local level and should now be expanded across Europe. Cyber research and development hubs on the campus will be instrumental in attracting and retaining such talent.

Build European standards. A European cyberproof label would raise awareness among users and promote the development of European cybersecurity capabilities. Cyber-proof labels already exist in countries such as France, but they should be promoted at a larger scale for standardisation. Each citizen should be part of the solution; cybersecurity should be embedded in Europe's DNA.

CONCLUSION

We think there are good reasons to be optimistic about Europe's prospects in the digital future. 5G is a technological turning point, and it presents an opportunity for fundamental change in the ways that digital services operate in the economy and wider society. In particular, Europe has an opportunity to regain sovereignty in a field that has till now been dominated by non-European companies.

Success will require action on a large scale, fast. Greater investment will be important but not sufficient. To succeed, Europe must find its own digital path, aligned with values such as cooperation and security. If Europe turns ideas into action, results will follow.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialised expertise in strategy, operations, risk management, and organisation transformation.

For more information, please contact the marketing department by phone at one of the following locations:

EMEA	Americas	Asia Pacific
+44 20 7333 8333	+1 212 541 8100	+65 6510 9700

AUTHORS

Emmanuel Amiot
Partner

Ivan Palencia
Partner

Augusto Baena
Partner

Charles de Pommerol
Principal