EXECUTIVE SUMMARY

Digitalization is revolutionizing our society transforming human existence, business models and the relationship between authorities and citizens.

Focusing on the European context, data shows that in the different Member States EU citizens and companies have a different level of computer skills and, more generally, a **different awareness of the advent of the digital age**, accessing available digital services with a different intensity and interest.

Chapter 1 provides a photograph on Internet usage, digital skills and digital service penetration in the EU. In particular, the analysis aims to describe some factors conditioning Internet usage (age, gender, Internet connection) and the most popular activities carried out online (par. 1.1.). At European level, data shows Northern Europe's primacy, a direct relationship between age and Internet usage and a greater interest of large companies - being more aware of digitalization's opportunities and having more resources to invest in the digital channel. Focusing on digital service penetration in Europe, par. 1.2.1. underlines that there are more than 4 billion people worldwide using the Internet, with the number of people using the top platform in each country increasing by almost 1 million new users every day during the past 12 months. **More than 3 billion people worldwide now use social media each month,** with 9 in 10 of those users accessing their chosen platforms via mobile devices. Globally, social media users have increased by 13 percent in the past 12 months.

The following paragraphs (1.2.2.) analyze e-commerce and Internet banking. Concerning **e-commerce**, it registered a new peak with **1.6 billion worldwide users who purchased products online and spending almost $ 2 trillion, an amount that could double by 2020.** Among the 10 countries with the highest penetration rates of online sales by mid-2017, we find China and South Korea (83%) at the top, followed by the United Kingdom (82%). Regarding the nationality of sellers, it's interesting to note that in 2017, in the European Union, **there was a preference for sellers from other EU countries** or within Member States. No big differences were shown between males and females while for age, individuals aged between 16-24 years and 25-54 years were more active in online shopping.

The **banking sector** (par. 1.2.3.) is also experiencing the digital revolution. Internet and mobile device penetration is reshaping the relationship between banks and customers, introducing new services and new ways of using traditional ones. **The highest percentage of users fall into the age groups of 25-34 year olds and 35-44 year olds**. **No gender difference was found in using Internet banking.**

The last paragraph of this chapter focuses on the value of the digital economy. **The value of the digital economy in terms of the contribution of**

information and communication technology to GDP growth is estimated to be around 5% of total GDP in the European Union.

The economic impact of the Internet is growing and has a huge potential in all European countries. In **Ireland**, the digital economy contributed to **10.7%** of the GDP in 2017, followed by Sweden and Luxembourg (7.2% and 6.8%, respectively), scoring above the EU average (Fig. 1.13). Instead, in the other European countries, such as Greece, Portugal, Austria and Italy, the contribution of the digital economy to GDP was lower than 4%.

Chapter 2 addresses the **cybersecurity threats** issue. The Internet allows people to connect worldwide and has led to the spread of a mass of smart devices for both individuals and businesses. However, this relatively new way of living (always accessible, everywhere at every moment) has resulted in many new problems in terms of security, and specifically cybersecurity.

According to the WEO, **cyber risks intensified** in 2017, so much so that cyber attacks and massive data fraud appear in the top five global risks perceived. Cyber branches have almost doubled from 68 per business in 2012 to 130 per business in 2017. **The financial costs of cyber attacks have also risen over the last five years** (+62%).

The recent cyber attacks have different and broader impacts compared to those incidents of the past decade. In 2017 alone, two major attacks involved **WannaCry** (in May) and **Petya** (in June). WannaCry hit, among others, the National Health Service in the United Kingdom, Nissan Motor Manufacturing UK and Renault. According to Cyence, the potential economic losses were estimated at $8 billion. Petya mainly hit the Ukraine, where the Chernobyl Nuclear Power Plant went offline, with an estimated loss of $850 million.

Cyber attacks have been changing over the last years. Until a few years ago, they were more focused (every week, a new retailer, healthcare provider, or financial institution lost their customers' sensitive data), while **now** these attacks **are more widespread, hitting, more or less simultaneously, several different companies and sectors worldwide**.

From 2013 to 2017, cyber crime, Cyber Espionage and Information Warfare have recorded the highest number of attacks. cyber crime has gradually increased from 53% to 76%, while hacktivist attacks have progressively decreased from 39% to 7%. Cyber espionage and information warfare increased in 2017 (by 47% and 24%, respectively).

Malware are the most widespread attacks accounting for a total of 787 million, of which 2.7% spread over the mobile network. Ransom attacks also increased, accounting for 12.5 million in 2017 (+226%).

European citizens are also facing the growing reality of cyber threats. According to Eurostat data, in the European Union, **the share of Internet users having experienced certain common security issues over the Internet** – such as viruses affecting devices, abuse of personal information, financial losses or children accessing inappropriate websites – was **25% in 2015** and is forecasted to increase in the coming years

if appropriate security measures are not implemented. Being infected by a virus or other computer infection was the main problem. In fact, **slightly more than 1 Internet user out of 5 (21%) in the EU caught an online virus or other computer infection resulting in a loss of information or time**. Moreover, security concerns prevented 24% of consumers providing personal information to online communities for social and professional networking; ordering or buying goods or services online (15%); downloading software, music, video files, games or other data files (15%); carrying out banking activities online (14%); or communicating with public administrations across the EU-28 in 2015.

Instead, among the European industries, **financial Services, fanufacturing and telecommunications are the main target of cyber criminals**, especially in Germany, Belgium, Spain and Great Britain.

The last paragraph of this chapter focuses on the regulatory framework; above all analyzing the initiatives carried out by the European Institutions to ensure **data protection.** These include: Regulation 679/16, the proposal for a regulation concerning the protection of individuals in the processing of personal data by EU institutions, authorities, offices and agencies, as well as free data movement; the proposal for a regulation on confidentiality and electronic communications; the proposal for a regulation of the European Parliament and Council on a framework for the free movement of non-personal data in the EU); **cybersecurity** (EU Cybersecurity Strategy launched in 2013; the Regulation on electronic identification authentication and signature; and Directive 2016/1148 - the NIS Directive - the strategic plan for cybersecurity launched in September 2017) in the European Member States.

Chapter 3 deals with **the impact of cybersecurity on enterprises**. Nowadays, cyber criminals are continually finding new ways to monetize personal information and many enterprises and organizations have been blackmailed. Furthermore, for some companies, intellectual property and trade secrets are their most valuable assets, and they now find these have become susceptible to new and growing threats. Therefore, the range of potential attacks and attackers is widening and increasing by the day. The new technologies, mobiles, and smart devices connected to the Internet of Things expose every organization to attackers and in an increasingly digitized world, cybersecurity has jumped to the top of companies' risk agendas after a number of high profile data breaches, ransom demands, distributed denial of service (DDoS) attacks and other hacks that have occurred over the last years. No sector of the economy is immune to attack; cyber criminals are increasingly targeting power grids, chemical plants, aviation systems, transportation networks, connected cars, telecommunications systems, financial networks, etc. Very often, **cyber crime uses very simple tools and tactics, namely emails, to make a big impact and to damage companies**. In fact, email is not just a communication tool but it is also one of the prime sources of threat for users and organizations. This threat can range from unwanted emails in the form of spam

to more dangerous types, such as the propagation of ransomware or phishing campaigns. According to the Internet Security Threat Report published by Symantec a growing proportion of spam contains malware. **Agriculture, forestry and fishing, together with the wholesale trade, were the sectors most affected by emails that contained malware in 2016**. In fact, the percentage of emails classified as malware was about 1% of the total. **Agriculture was also the sector most affected by phishing in 2016**, with 0.06% of emails classified as phishing attempts followed by the finance and insurance sectors.

The main and most costly impacts on organizations that suffer a cyber attack are business disruption, loss of information, loss of revenue and damage to equipment. According to the global survey conducted by Accenture and the Ponemon Institute (2017), for 43% of the organizations interviewed, **the most damaging consequence was the loss of information**. Instead, **business disruption was mentioned by 33% of organizations** and, **finally, revenue losses and equipment damages were reported by 21% and 3%, respectively**.

To reduce cyber risks, the companies have had to adopt cyber risk mitigation measures and ICT security policies. A cybersecurity program should include at least three elements: training employees to recognize phishing attempts and malicious emails; restricting access to key data and information; and preparing an incident response plan and identifying key vendors before a cyber event. According to the global survey conducted by Kroll (2018), **the most implemented actions are employee restrictions on installing software (89% of respondents) and employee cybersecurity training (83% of respondents)**. Incident response plans (IRPs) also lead the list, with 80% of respondents indicating their company already has an IRP in place.

Instead, the top three actions the IT companies should implement in the next months are intrusion detection systems that are device-based, endpoint threat monitoring and intrusion detection systems that are networked based.

As far as Europe is concerned, **in 2015, almost one out of three enterprises in the EU-28 had ICT security policies in place**. **The issue of cybersecurity is particularly felt in large companies** and more than 70% of European large companies adopted an ICT security policy in 2015, while less than 1 in 3 SMEs had done so. Finally, **ICT and professional, scientific and technical activities are the main sectors that show interest in the cybersecurity issue** with 62% and 49%, respectively, of European enterprises defining IT security policies

Moreover, cloud computing has entered the mainstream of information technology, providing scalability in the delivery of enterprise applications. It provides improved efficiency in everyday tasks, as well as a pathway for massive amounts of data generated by IoT to travel.

At a European level, the adoption is still quite weak – just one in five European companies use a cloud

computing service, and just 14% make use of more sophisticated cloud computing services. Nonetheless, at a global level, the trend is definitely growing, and Europe cannot but fall into line.

Among the main **benefits** identified by enterprises are a **faster access to infrastructure** (62% of interviewees), **greater scalability** (61%), **higher availability** (56%) and **faster time-to-market** (51%). However, the cloud also involves challenges. These include a lack of resources and expertise, with security and managing cloud spending being the most compelling ones, although the latter has been gradually decreasing.

Companies should decide, based on their needs and capabilities, which cloud model fits best with their internal organization, choosing from among private, public or hybrid cloud models. That said, however, while adoption of the public cloud has been limited to date, future prospects seem to be markedly different and, today, many companies are moving towards public cloud solutions. This is mainly due to its ease of scalability (implying a high degree of cost-effectiveness) and also to its greater reliability, since it involves a vast network of servers, thus redistributing the load among the other data centers, should one center fail. According to the results from a recent McKinsey study, although just 40% of the companies studied has more than 10% of their workloads on public cloud platforms, about 78% are planning to increase this to more than 10% within three years or to double their cloud penetration. In addition, the worldwide public cloud services market revenue was projected to grow by 18.5% in 2017 to a total of $260.2 billion, up from $219.6 billion in 2016, and is expected to reach $411.5 billion by 2020.

As enterprises scale up their use of the public cloud, they must rethink how they can protect data and applications. In particular, they need to dramatically evolve their cybersecurity practices in order to consume public cloud services in a way that enables them both to protect critical data and to fully exploit the speed and agility that these services provide. Security is often cited as one of the top barriers to cloud migration. For this reason, companies need a proactive, systematic approach to adapting their cybersecurity capabilities for the public cloud. This approach is described in a detailed manner in section 3.4.3. In addition, **a model of Security as a Service is recently emerging. It is an outsourcing model for security management that does not require on-premise hardware and entails**, among others, **two main benefits: constant virus definition updates that are not reliant on user compliance and greater security expertise than is typically available within an organization.**

The real matter is that applications and data maintained in the cloud can be more secure than data held in on-premise corporate systems because **moving to the right kind of advanced cloud system represents a more dynamic approach to risk**. As companies digitize more and more aspects of their internal operations and external contacts, the standard approach involving the use of IT systems to detect and prevent unwanted efforts to gain entry becomes no longer effective. The problem calls for an

entirely different type of solution and the cloud may offer several benefits. In particular, **it can provide almost unlimited low-cost computational power**, which is often needed to identify suspicious activities, something that is impossible for traditional IT systems when it comes to monitoring huge volumes of data and highly complex and interconnected applications. Furthermore, **it is able to detect and respond to intrusion more dynamically, with a learning capacity that traditional IT technologies don't have**. The final strength of the cloud-based system lies, thus, in its ability to combine authentication and analytics from multiple sources. As cyber attacks become an increasingly shared problem, with a cloud-based system we can openly exchange information about the attackers' identities and the nature of the threats they pose, resulting in a shared knowledge base without compromising anyone's secure data.

Chapter 4 provides for a focus on three industries - manufacturing, energy and automotive.

For manufacturing, the IoT is at the center of the industrial transformation because of the revolutionary ways this connected technology has streamlined and simplified various manufacturing processes. Traditionally, robots have been used to perform tedious, repetitive tasks on the assembly line. Today, they are capable of mimicking more human traits, such as dexterity and memory, of providing safer working environments, as well as valuable feedback and data, thus allowing companies to make necessary adjustments more accurately. Within the EU, Germany and Italy are the two largest markets – 5th and 7th at a global level -, 36% and11%, respectively, of the overall EU market, numbering 56,000 robots sold in 2016 and expected to reach 82,600 units by 2020. **As manufacturers innovate cyber threats accelerate and become more and more sophisticated**. According to the results of a study by Deloitte and the Manufacturers Alliance for Productivity and Innovation (MAPI), **top threats**, damaging about one third of the interviewed enterprises, **include IP theft (34%) and phishing/ pharming (32%).** In addition, increasing dependence on technology-enabled connected products brings a new set of risks to manufacturers such as attacks involving mobile devices or mobile networks, that concern about one in four surveyed companies.

The challenge of implementing a secure, vigilant, and resilient cyber risk strategy is different in the age of Industry 4.0. One major problem is machine obsolescence that, once combined with connected devices, become particularly vulnerable. In addition, cybersecurity should become an integral part of the strategy, design and operations, being considered from the beginning of any Industry 4.0 – driven initiative. **A first important step is to provide the company with a formally written security policy, however,** across the EU countries, only one in three manufacturing companies has done this. Sweden ranks first among the EU countries with a 53% of manufacturing companies equipped in this sense, followed by Italy (45%). **Another major problem is the multitude of products and vendors in manufacturing settings,**

that creates a confusing picture for security experts. 46% of the manufacturing security professionals said they use six or more security vendors, and 20% more than 10 vendors. In addition, security is often outsourced, especially among small and medium-sized businesses (SMB). **Another hurdle is represented by the composition of security teams**. Nearly 60% of the manufacturing organizations said they have fewer than 30 employees dedicated to security and 25% complain about a lack of trained personnel. Finally, **manufacturers also need their IT and OT departments to share knowledge**, so as to reduce to a minimum the consequences of one's processes or downtimes on others. What companies are currently focusing on is mainly application security involving the use of software, hardware, and procedural methods to protect applications from external threats (41% of interviewed companies), as well as, security consultants (38%) and the use of anti-viruses (38%).

The cloud will lead also in manufacturing. At the manufactured-product level, cloud computing will transform everything from how products themselves are researched, designed- and developed, to how they are fabricated, manufactured and used by customers in the field. Moreover, it will play a key role towards enabling and democratizing new manufacturing production systems such as 3D printing, generative design and the Industrial Internet of Things.**Today, digital services such as cloud computing provide at least 25% of the total input that go into finished manufactured products**. One particularly important benefit of the **cloud** is that it **allows manufacturers to leverage infinitely scalable computational resources**, so that they can readily access the computational resources they require without having to purchase expensive IT equipment up-front. This is **especially important for small and medium-sized manufacturing enterprises (SMEs) that lack the financial resources to purchase expensive IT equipment.** Summing up, cloud computing is helping manufacturers innovate, reduce costs and increase their competitiveness. It allows for the use of many forms of new production systems, from 3D printing and high-performance computing (HPC) to the Internet of Things (IoT) and industrial robots, democratizing access to and use of these technologies by small manufacturers.

The security aspects are very important when cloud computing is used given that **the security strategies that have been developed so far are not suitable**. **This is probably the reason why the degree of adoption of cloud computing services – especially those of medium and high level of sophistication - is still quite low across EU manufacturing enterprises (17% and 9%, respectively).** However, one major benefit associated with cloud computing, according to some, is that it can actually make manufacturing IT systems more secure. This is because **cloud-computing providers employ best-of-breed cybersecurity practices that are often far more sophisticated than what individual companies can achieve by themselves** on a one-off basis, which is particularly true for SMEs lacking the needed resources

and expertise. **Thus, cloud computing may represent an opportunity to have better data security at affordable prices**.

The **growing digitalization** of the economy has also exposed the energy sector to cybersecurity risks. **Utilities are increasingly exposed to IT risks**, due to the **smart electricity** networks with thousands of interconnected users. As other companies, utilities are threatened by economic cyber risks (e.g. a hacker wishing to profit from an attack, by diverting money to an account or stealing industrial information). However, the main concern for energy companies is relevant to the cyber attacks that could affect electricity generation plants and transmission grids.

Although utilities were among the first companies to computerize, today the **need for a renewal** has emerged. Many utilities use **equipment** that works very well from an industrial point of view, but they are **obsolete from an IT point of view** (e.g. old control systems).

Cybersecurity is becoming a priority in the energy sector so that, in 2015, **40% of European energy companies had already formally adopted an ICT security policy**. Among risks, energy companies are less worried by the unavailability of ICT services due to an attack from outside (e.g. Denial of Service attack), with only 29% of European enterprises having formally defined a specific ICT security policy against this cyber threat. While 37% are concerned about data destruction or corruption resulting from an attack or unexpected incident.

Following the description of the four energy **cybersecurity priorities** by the EECSP-Expert Group[1], the study addresses two topics that from the point of view of cybersecurity can be seen as a strength or as a weakness - smart grids and the cloud.

Smart grids have a huge potential in terms of safety, productivity, improvement of service quality and operational efficiency, despite **requiring more care** in terms of cybersecurity. A distributed energy system unquestionably has a **higher number of potential vulnerabilities** and access points. However, the **effects** and the **impacts** of possible attacks **can be reduced and isolated to a specific part of the system**. It is therefore **crucial to establish an adequate security system**, in order to safely carry information on the digital network and prompt reply malfunctions and interruptions in the electricity supply. Due to the possible impact of a successful attack on consumer trust and the rise in security questions along the value chain, smart grids should be equipped with sophisticated protection mechanisms that can evolve rapidly and adapt to the continuous development of malware.

Thanks to the evolving energy paradigm – increasingly focused on **decentralized model** and **energy storage systems**, as well as electricity **producers and consumers**, **all working together through remote control and monitoring** as virtual power plants –

1 Identified priorities:
- to formalize an effective threat and risk management system at EU level
- to establish an effective response framework at regional level
- to boost the improvement of cybersecurity resilience
- to make available adequate energy cybersecurity skills and competences.

the energy cloud is becoming increasing important. Supported by technological progress, it encompasses platforms to enable the matching of traditional market players and customers. In 2016, **19% of European energy enterprises used at least one of the cloud computing services**. Finland and Sweden were the most active in the energy cloud, 49% and 44%, respectively. Looking at the type of services used[2], 9% of European energy enterprises used high cloud services. The best performers in the use of high cloud services were Finland (34%) and the Netherlands (27%). **Many cloud experts believe that trusted cloud data centers have better security than in-house data centers**. From this point of view, security is contingent upon the reliability of the provider. Therefore, although the main reason for adopting the cloud was not originally for security, security itself could become a key success factor for cloud computing companies.

The study also showed some attacks recently occurred in the energy sector, a tiny part of all occurring cyber incidents.

Concerning **cybersecurity in the automotive sector, the number of connected vehicles** in the world is constantly increasing. According to some estimates, connected vehicle installations in China, North America, Europe and Japan **should reach 68 million by the end of 2018, an increase of 278% compared to 2013. Autonomous vehicles** of level 4 and 5 **will begin to mainstream after 2028 and the analysts forecast about 80 million level 4 and 5 autonomous cars in China, North America and the European Union by 2030**.

Connected and autonomous cars take us toward a mode of transport that is more efficient, by enabling an interconnected driving experience but there is concern because **interconnecting via Internet could expose vehicles – and the people in them – to potential risks from online threats.** The cybersecurity risk for connected cars is of particular importance because external access to a car's network not only compromises the privacy of a driver's data, but also the cybersecurity threat to connected cars can become a matter of life and death, threatening the industry's road map towards autonomous and connected vehicles.

According to the results of a survey (Foley, 2017) conducted on 83 automotive and technology executives between America and Asia, **IT security and privacy - selected by 31% of respondents - are an important concern for connected cars and the main obstacle to their development**. In addition, **cybersecurity attacks emerged as the top legal issue for 63 % of respondents** that must be addressed in developing technology for connected cars and/or autonomous vehicles. **Not only companies but also consumers are worried about cybersecurity in connected cars**. The Irdeto Global Consumer Connected Car Survey examined consumer awareness of cyberattacks targeting connected cars and autonomous vehicles and,

2 According to the Eurostat ranking there are three levels of services:
- Low: email, office software, storage of files;
- Medium: email, office software, storage of files, hosting of the enterprise's database;
- High: accounting software applications, CRM software, computing power.

according to this survey, **85% of global consumers indicated that they believe any connected car has the potential to be targeted by a cyber attack and 59% of connected car owners are concerned that their vehicle could be targeted by a cyber attack**.

After describing of the concerns about cybersecurity in the automotive sector, the study addresses the topic related to the role of cloud computing. Cloud-based services offer new navigation systems to drivers and passengers. Moreover, cloud connectivity is also changing infotainment and supporting the evolution of autonomous driving and can help automotive companies to redefine and personalize customer relations and transform and optimize operations. Furthermore, the cloud ensures the cutting edge technology to improve **its performance in cybersecurity through platforms able to hinder any cyber attack attempts**.

Only through the thoughtful use of disruptive technologies such as big data, machine learning, artificial intelligence and the use of cloud computing can we help build a better, safer and more secure connected vehicle ecosystem.