# Engineering Resilience

## Current Challenges, Risks and Recommendations for the Information and Communication Technology Sector in Europe

efca
European Engineering Consultancies

# Content

# Foreword

The resilience of the European ICT sector, and particularly of its infrastructure, is a critical factor in ensuring the continent's socio-economic stability and competitiveness, as well as in achieving its climate ambitions. This document has been produced by EFCA's Future Trends Committee in association with the University of Marburg. It provides a comprehensive analysis of the current state of the European ICT sector, identifying key vulnerabilities, and proposing strategic solutions to enhance its resilience. It highlights the consulting engineering sector's vital role in addressing some of its structural and operational challenges, mitigating geopolitical and climate-related risks, and ensuring a sustainable future for Europe. With a number of recommendations also addressing the relevant parts of the EU legal framework for ICT, we hope that this paper, part of our annual Future Trends Report, will stimulate further dialogue with EU and national policy makers and we look forward to sharing EFCA's expertise at this pivotal moment. Due to the recent rise in threats, particularly cyberattacks, the importance of shoring up our ICT infrastructure and improving the overall European ICT ecosystem cannot be overstated. I would like to extend my gratitude to all the contributors who have dedicated their time and expertise to this important work, which are listed below. Their invaluable insights and collaborative efforts have been instrumental in shaping this comprehensive study.

***Jeffrey Seeck***
*Chair of the EFCA Future Trends Committee*

## EFCA FUTURE TRENDS COMMITTEE MEMBERS

**Nikola Matić** (ACES - Serbia)

**Iana Motovilnic** (ARIC - Romania)

**Pavlina Mladenova**
(BACEA - Bulgaria)

**Emmanuelle Frénéat**
(CINOV/SYNTEC-Ingénierie - France)

**Anders Persson**
(FSIC – Innovationsföretagen - Sweden)

**Despina Kallidromitou**
(HELLASCO - Greece)

**Maddalena Rostagno** (OICE - Italy)

**Alexandre Vanheule** (ORI - Belgium)

**Richard Opsahl Resvoll**
(RIF - Norway)

**Marcin Mikulewicz** (SIDiR - Poland)

**Inés Ferguson** (TECNIBERIA - Spain)

**Ralf Bufler** (VBI - Germany)

**Maximilian Grauvogl**
(VBI - Germany)

## CONTRIBUTING ADVISORS

**Andreas Bach** (Schüßler Digital Plan/VBI)

**Andreas Schweinar** (Yorizon)

**Andrew Pidgeon** (Dorsch Global/Queens University Belfast)

**Nikola Matić** (ACES - Serbia)

**Pierluigi Bassetto** (NESA)

**Torsten Wulf** (Phillips-University Marburg)

## CONTRIBUTING AUTHORS

**Friedericke Hössle** (Phillips - University Marburg)

**Lucas Cornaro** (Phillips - University Marburg)

**Mihai Barcanescu** (EFCA Secretariat)

## CHAIR OF THE EFCA FUTURE TRENDS COMMITTEE

**Jeffrey Seeck** (VBI - Germany)

# Executive Summary

## OVERVIEW OF THE SECTOR'S CURRENT STATE

The ICT sector is at different stages of development in its various sub-sectors in Europe. Some areas still require further development:

1. Gigabit internet infrastructure: the EU's Digital Decade 2030 targets (European Commission, 2025c) set the goal of providing gigabit connectivity to all European households by 2030. While gigabit-capable coverage reached about 82.5% of the population in 2024, at the current pace the target will not be met, with projections suggesting only 90% coverage by 2030. Achieving full coverage will require an estimated €174–200 billion in additional investment;
2. 5G rollout: the Digital Decade also requires 5G coverage for all populated areas by 2030. As of 2024, overall 5G coverage stood at around 81–87%, but only ~51% in rural areas. Furthermore, 5G standalone (SA) networks, which are essential for advanced applications, are used by just 2% of users in Europe, compared to a much higher adoption in the US (24%) and China (77%);
3. Cloud and edge computing: the EU lags behind its own expansion targets, which aim for 75% of EU enterprises to adopt cloud services, big data and AI by 2030. Current adoption is progressing, but still falls short of the expected trajectory;
4. Resilience and cybersecurity: different measures have been taken to strengthen resilience, including the Digital Operational Resilience Act (DORA), the second Network and Information Systems (NIS2) Directive, the Critical Entities Resilience (CER) Directive and the Cyber Resilience Act.

## IDENTIFICATION OF KEY VULNERABILITIES

The sector's resilience is hampered by vulnerabilities:

1. One major vulnerability is the ageing physical infrastructure, such as mobile networks and undersea cables;
2. Furthermore, Europe simply lacks the specialised ICT personnel who could drive forward the field of cybersecurity;
3. The lack of investment in the market is further limited by fragmentation and excessive government regulation, as noted by the EC in its report State of the Digital Decade 2025, which encourages the relevant stakeholders to keep building the EU's sovereignty and digital future;
4. One vulnerability that could also be turned into a strength is the increasingly strong interdependence of the ICT sector with other critical infrastructures, such as water, transport and energy.

## SUMMARY OF GEOPOLITICAL AND CLIMATE THREATS

Geopolitics poses a major threat to ICT, and climate change should not be forgotten either:

1. One of the greatest risks, which is becoming even more critical due to increasing geopolitical tensions, is Europe's heavy dependence on foreign technology providers, infrastructures and platforms. This includes reliance on US hyperscalers for cloud services, Asian suppliers for semiconductors, and Chinese vendors for critical raw materials and telecom equipment, which are exposures that leave Europe strategically vulnerable;
2. Supply chains pose an ever-growing threat. They are increasingly subject to attacks and sabotage attempts;
3. Cyber threats are a major issue in ICT. These attacks are becoming more frequent, especially amid geopolitical tensions;
4. The sector's physical infrastructure is suffering from the increasingly severe effects of climate change.

## PROPOSED SOLUTIONS AND RECOMMENDATIONS

It is precisely because of these risks and weaknesses that it is urgently necessary to build greater resilience:

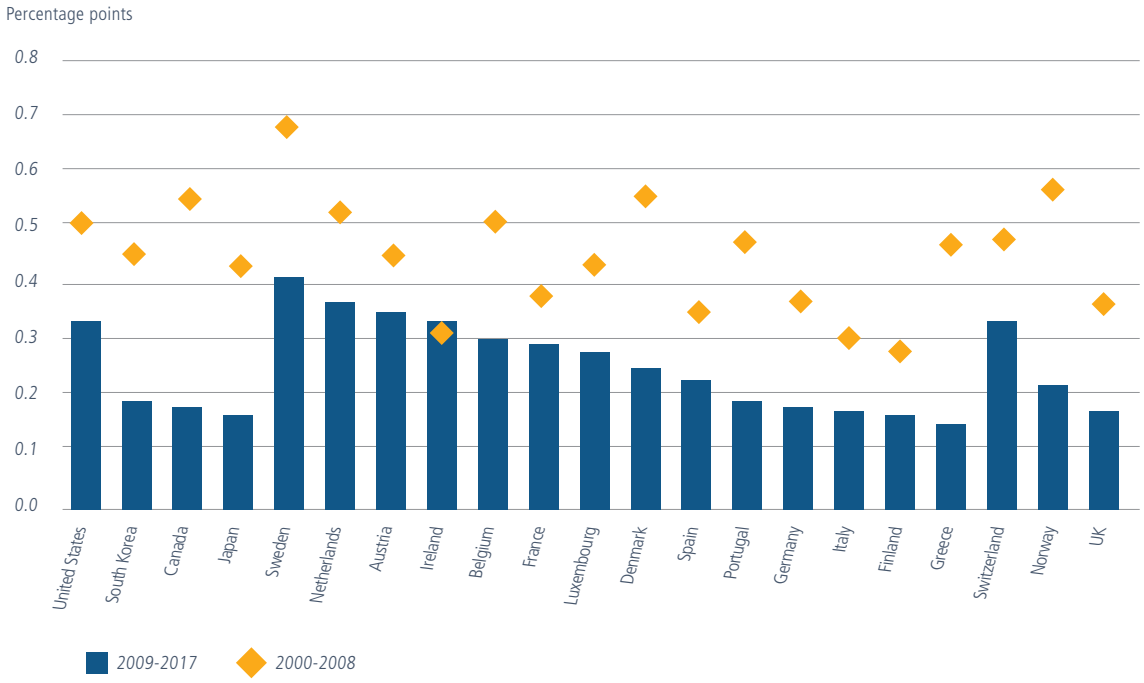
1. Resilience measures must be incorporated into the system architecture at an early stage;
2. Various techniques for increasing resilience should be combined, rather than implementing just one;
3. Sensor fusion and analysis methods can be used to detect threats in real time;
4. Research and development should be increased through the right financial and non-financial incentives, including direct and indirect tax incentives, where necessary;
5. Digital skills and the promotion of ICT specialists should be significantly boosted through education policy with targeted measures.

# Introduction

## PURPOSE OF THE REPORT

Part of the Information and Communication Technology (ICT) sector's infrastructure is considered critical infrastructure in Europe because of its key contributions to the functioning of other critical infrastructure such as energy, transport, finance and health. This means that the proper functioning of these essential services is critically dependent on ICT technology (European Commission, 2024d). A malfunction or disruption in communication channels or IT systems can trigger a cascading effect across other infrastructure or services, potentially affecting all of Europe. The ICT sector thus forms its own critical infrastructure, consisting of the internet, telecommunications and IT Systems.

**Figure 1. Contribution of ICT capital to GDP growth (8 percentage points) over 2000-2008 and 2009-2017. (EC Europa, 2020, p. 340)**



Therefore, strengthening the resilience of the ICT sector is crucial due to a dynamic and evolving threat landscape and inherent vulnerabilities.

## RELEVANCE OF THE SECTOR

ICT is crucial for Europe, including security, economy and sustainability, due to its fundamental role in modern society and its potential to drive positive transformation.

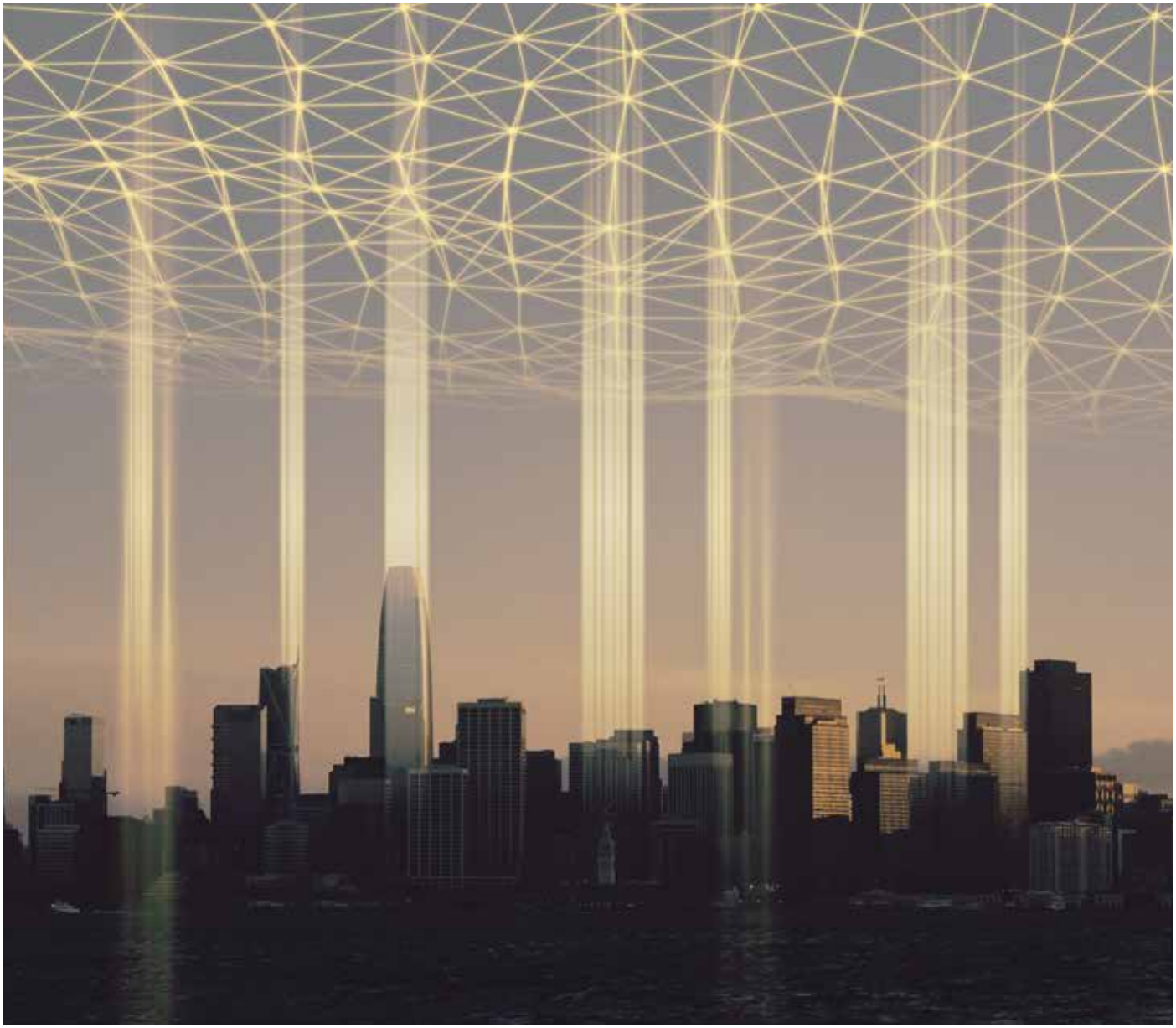
Modern ICT systems are indispensable to Europe's digital transformation, but they also introduce new vulnerabilities. The benefits of the European digital economy and society can only be fully attained under the premise of a high and common level of cybersecurity. Cybersecurity has therefore become a structural requirement for critical sectors, enhancing the trustworthiness of digital products and services and preparing Europe to respond to cross-border cyber threats and incidents (The EU Agency for Cybersecurity – ENISA).

A major source of economic growth for the European Union is ICT, with the potential to contribute significantly to GDP growth (see Figure 1) if the Single Market is deepened and new technologies are fully embraced (European Commission, 2014). To avoid falling behind global competitors, Europe urgently needs to realise its full ICT potential as it mobilises innovation and services for jobs and economic recovery.

Technologies like robotics, the Internet of Things, Artificial Intelligence (AI) and data analytics are expected to have a significant impact on the built environment in numerous ways, e.g. by making waste management more efficient, from optimising collection logistics to automating sorting processes that are vital for high-level recycling.

The following pages analyse the risks and threats facing the ICT sector in Europe and emphasise the importance of greater resilience in this critical infrastructure.

# Current State of the Sector



## OVERVIEW OF THE SECTOR

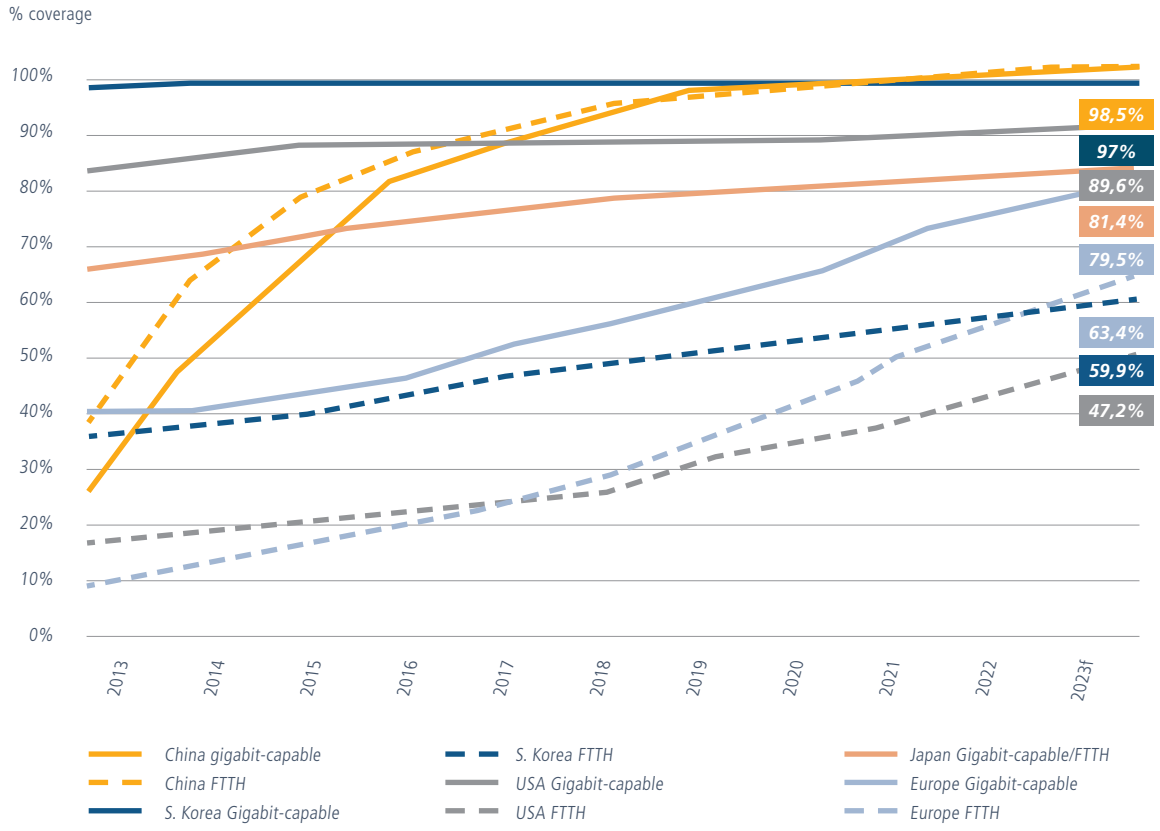
First, we will look at the area of internet connectivity in Europe.

By 2023, Europe's gigabit-capable coverage (coverage of 1000 Mbps) reached 79.5% of the population, increasing to an estimated 82.5% in 2024 (Connect Europe, 2024). This still trails South Korea, the USA and Japan (Connect Europe, 2025).

'Fibre To The Home' (FTTH) coverage specifically reached 63.4% in 2023 (Connect Europe, 2024), growing to an estimated 70.5% in 2024, which is notably better than South Korea and the USA (Connect Europe, 2025). (See Figure 2).

Despite this progress, it is estimated that at least 45.4 million people in Europe (39.5 million in the EU alone) will still lack access to a fixed gigabit connection by 2030, falling short of the Digital Decade target, which stipulates that all European households should have access to a fixed gigabit connection by 2030 (Connect Europe, 2025). This also means that some businesses, mostly (smaller) SMEs, will be left out. An additional €109 billion of investment in FTTH alone is required to reach 99% of the European population by 2030. Of the remaining cost to achieve 99% FTTH coverage,

**Figure 2: Gigabit-capable and FTTH population coverage, China, Europe, Japan, South Korea and the USA, 2013-2023. (Connect Europe, 2025, p. 15)**



about 45% would need to come from public funds (Connect Europe, 2025). However, EFCA members have also pointed out another challenge on this aspect: national authorities will also need to focus more on the high-capacity network/ infrastructure in the key areas, which is either ageing or not properly protected, or both. This is a key concern not only for the areas directly served by these infrastructure segments, but also for the functioning and expansion of the entire national infrastructure.

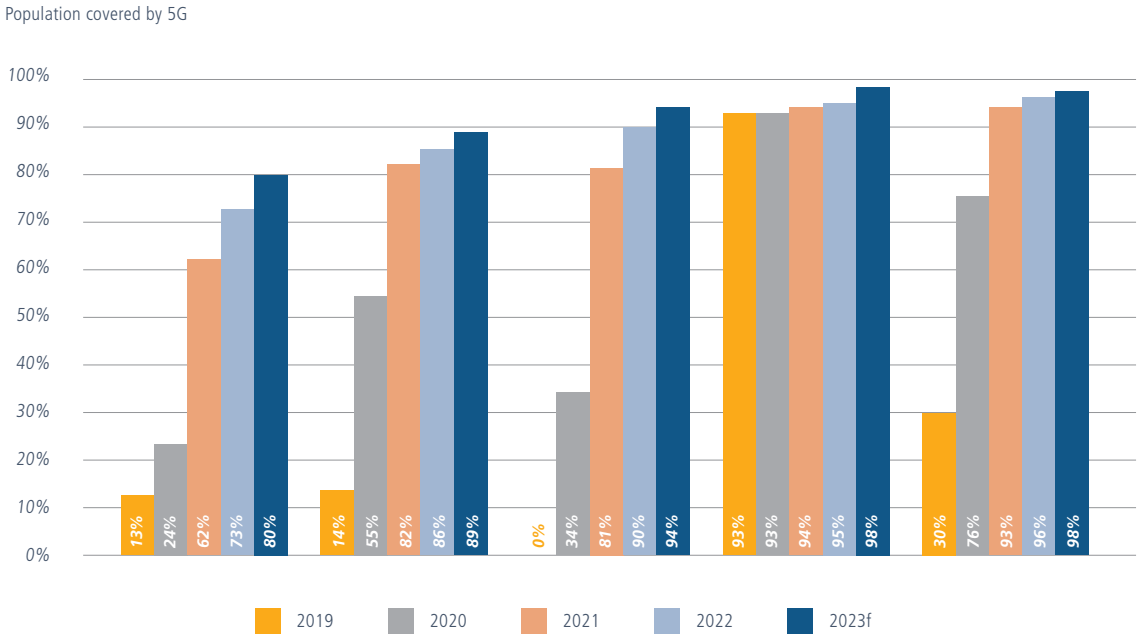
The second area of the sector to be examined is telecommunications. An important part of this is mobile broadband.

5G coverage in Europe reached 80% of the population in 2023, an increase from 73% in the previous year (Connect Europe 2025). However, Europe still trails global leaders such as South Korea, the US, Japan and China (Connect Europe 2024). This can be seen in Figure 3. Rural 5G coverage saw a significant rise from 51.0% to 73.7% between 2022 and 2023 (Connect Europe 2024).

Despite mobile data usage levels evening out with global peers, Europeans consistently spend less per capita on telecoms compared to the USA, Japan and South Korea, with revenue per used gigabyte of mobile data in the USA being 159% higher than in Europe (Connect Europe 2025). This revenue gap creates pressure on European telecom operators but also opens opportunities for the ICT industry to innovate in efficiency, resilience and service differentiation. In particular, consulting engineers can play a key role in strengthening critical infrastructure by optimising network rollouts, integrating energy-efficient technologies and designing more resilient systems that help operators remain competitive under tighter financial conditions.

The final component of the ICT sector is represented by the main IT systems. This also includes cloud systems and edge computing.

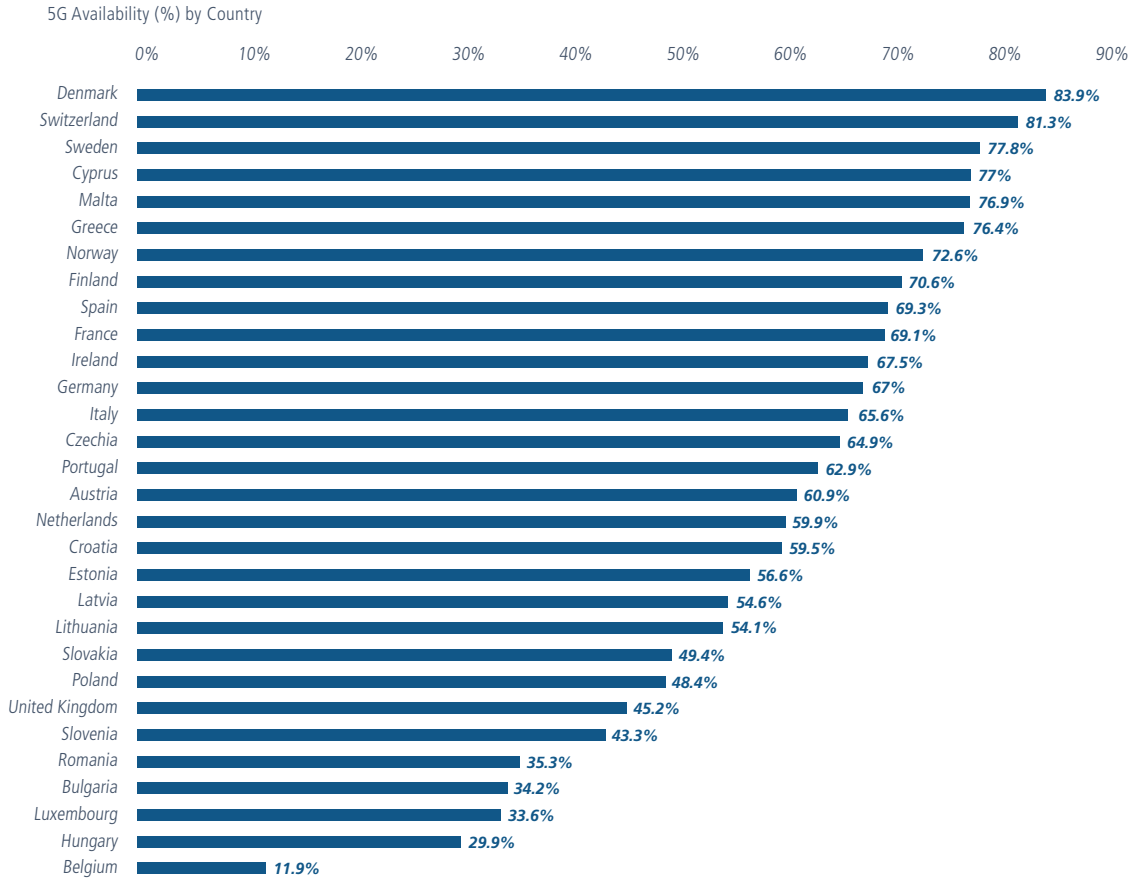
**Figure 3: Percentage of the population covered by at least one 5G mobile operator, 2019-2023. (Connect Europe, 2024, p. 18)**



The European cloud computing market was valued at over €110 billion in 2023 and was projected to reach €129 billion by 2024 (Rolling Plan for ICT standardisation, 2025). Cloud computing refers to the on-demand delivery of IT resources - such as storage, computing power, and software - over the internet, enabling enterprises to scale services flexibly without owning the underlying infrastructure. In 2023, 45.2% of EU enterprises used cloud computing, primarily for email, file storage and office software, showing a 4.2 percentage point increase from 2021 (Rolling Plan for ICT standardisation, 2025; European Commission, 2024a). The EU's Digital Decade 2030 goal is for 75% business cloud adoption (European Commission, 2024a).

Edge computing refers to the practice of processing data closer to where it is generated - such as in devices, sensors, or local edge nodes - rather than sending all data to centralised data centres or clouds. This reduces latency, saves bandwidth, and enables real-time applications. Edge computing is expected to process a growing proportion of data where it is generated (Connect Europe, 2024). By the end of 2023, the EU27 had over 1100 edge nodes deployed by various entity types, with operators having deployed around 320 (Connect

**Figure 4: 5G Availability across Europe. (Kehoe, 2025)**



Europe, 2025). The Digital Decade 2030 target is 10,000 climate-neutral and highly secure edge nodes across Europe, indicating a long way to go (European Commission, 2024a), (Rolling Plan for ICT standardisation, 2025). While the diversity of actors deploying edge nodes reflects a dynamic and innovative ecosystem, it also creates fragmentation and challenges for interoperability, security and climate neutrality. With just over 1,100 nodes deployed against the 10,000 target, Europe risks falling behind unless coordination and scaling accelerate significantly.

## REGIONAL VARIATIONS

Europe exhibits significant regional differences in its ICT sector. This "two-speed" competitiveness landscape is influenced more by national policies than by geography or demographics (Kehoe, 2025).

Differences can be seen, for example, in 5G coverage and availability.

As of Q2 2025, Nordic and Southern European countries, such as Denmark, Sweden, and Greece, maintain a substantial lead in 5G availability (Kehoe, 2025). Their coverage rates are up to twice as high as those in Central and Western European laggards like the United Kingdom, Hungary and Belgium (Kehoe, 2025). (See Figure 4).

One can also see differences between the various regions and countries in Europe based on market size. The United Kingdom dominated the Europe IT services market with a 28.7% revenue share in 2023 (Europe IT Services Market Size & Trends, 2024). The UK, Germany, and France are expected to account for around 51% of total IT spending in Europe in 2024, reaching $588 billion, a 9.8% increase over 2023 (Silicon Editorial, 2023). Italy's digital market is also experiencing remarkable growth, projected to reach €91.7 billion in 2025 (ICT, 2025).

Nicola Matić (2025) pointed out another difference in an interview: the varying understanding of ICT and its components among different generations. He emphasises the importance of *"having a mutual understanding about the ICT we are talking about."* Through an exchange between these different understandings, new experiences and solutions can then be gained.

## EXISTING POLICY RESILIENCE MEASURES

Due to the increasing number of threats to critical ICT infrastructure, various programmes and initiatives have been launched to strengthen resilience.

The first EU legislation to address ICT infrastructure across the EU was that of the trans-European networks (TENs) in transport, energy and telecommunications. This was developed to connect the regions of the EU and to contribute to market and employment growth. In the case of telecommunications, Decision 1336/97/EC of 1997 laid down guidelines for the trans-European telecommunications networks (TEN-Telecom). The priorities adopted included applications contributing to economic and social cohesion and the development of basic networks, particularly satellite networks. Over time, both the legislative framework and the needs on the ground evolved, and the investments shifted more towards the modernisation of existing telecom networks (European Parliament, n.d.). Since 2014, most of this work is done via the Connecting Europe Facility (CEF) (HaDEA, 2025). The TEN-Telecom and CEF frameworks are important because they offered the first European approach to key elements of ICT infrastructure, starting with harmonised, high-level quality requirements for both greenfield and brownfield infrastructure projects, subsequently followed by the incorporation of climate-resilience and cybersecurity aspects. The trans-European transport network (TEN-T) and the energy

infrastructure network (TEN-E) also have a role in this case, since their infrastructure projects also prescribe the inclusion of modern ICT components (e.g. ETCS and ERTMS for railways) and the climate resilience and cybersecurity aspects.

A unified legal framework to uphold cybersecurity in 18 critical sectors across the EU is provided by the Network and Information Systems Directive 2 (NIS2). It replaced its predecessor, NIS1, to respond to increased cyber threats and raise the common level of cybersecurity ambition in the EU (NIS2 Directive, 2024). NIS2 mandates Member States to enhance their cybersecurity capabilities, implement risk management measures, and impose reporting requirements on entities from more sectors (NIS2 Directive, 2024). NIS2 came into force in January 2023, and Member States were required to transpose it into national law by October 17, 2024 (NIS2 Directive, 2024).

Closely linked to NIS2 is the Directive on the Resilience of Critical Entities (CER Directive), which entered into force in January 2023, and its supplementing Delegated Regulation (2023). While NIS2 focuses on cybersecurity, the CER Directive addresses the physical and organisational resilience of critical entities across 11 sectors, including energy, transport, health and digital infrastructure (CER Directive, 2023). More specifically, the Directive lays down obligations for EU Member States to take specific measures to ensure that essential services for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner. It thus created an overarching EU-level framework that addresses the resilience of critical entities in respect of all hazards, whether natural or man-made. However, each country defines its own list of critical entities, based on the geopolitical, economic, etc. context, therefore there is no unified list of these critical entities at EU level. The Delegated Regulation establishes the non-exhaustive list of essential services that are covered by the CER Directive. One of the identified sectors is digital infrastructure, and some of the services explicitly mentioned include: provision and operation of internet exchange point service, provision of cloud computing services, provision of data centre service, etc. Together, the two Directives and the Regulation create a more integrated framework to safeguard Europe's critical infrastructure against both cyber and non-cyber risks.

The Cyber Resilience Act (CRA) is the first EU Regulation to establish a minimum level of cybersecurity for all connected products available on the EU market. It applies to everything from low-cost consumer devices (such as smartphones, smart home products and internet-connected toys) to B2B software and complex industrial systems. Importantly, the CRA applies not only to EU manufacturers but also to distributors and importers of digital products (Cyber Resilience Act, 2024).

In addition, the Digital Operational Resilience Act (DORA) strengthens the resilience of financial entities, such as banks, insurance companies and investment firms, along with their ICT third-party service providers. Applicable since January 17, 2025, DORA ensures that these entities can withstand, respond to and recover from ICT disruptions, including cyberattacks and system failures. It harmonises rules for operational resilience across 20 different types of financial entities and ICT providers (DORA, 2025).

Lastly, it should also be mentioned that there is a significant interconnection between the GDPR rules and cybersecurity, because the GDPR serves as a catalyst for improving cybersecurity standards by requiring organisations to assess their data processing activities and implement robust security measures.

# Vulnerabilities Assessment

## STRUCTURAL WEAKNESSES

### Ageing physical infrastructure

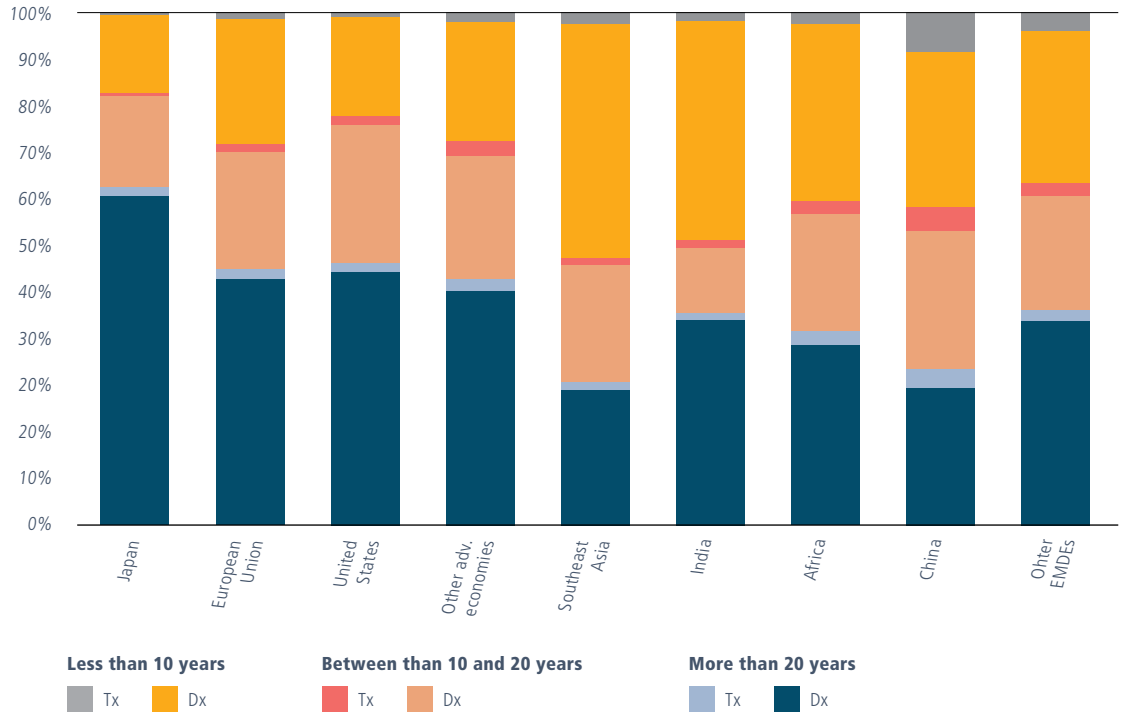
One of the most pressing structural weaknesses is the ageing digital infrastructure, which is straining service providers both financially and operationally (Wodecki, 2025). Many telecommunication operators (telcos) admit that legacy networks, such as copper, 2G and 3G are slowing the rollout of new services while increasing operational costs (Wodecki, 2025). For instance, 81% of surveyed telcos believe legacy networks hinder new service deployment, and a significant portion expect copper networks to remain operational until at least 2028, with 2G lasting until 2030 or beyond (Wodecki, 2025). This continued reliance on older infrastructure is a major hurdle to innovation in 5G and fibre, undermining competitiveness and sustainability (Wodecki, 2025). Some countries can move forward more quickly due to their financial resources and/or political will, at least in some segments (e.g. France), yet the overall problem remains.

Another area of infrastructure that is ageing and underdeveloped is submarine data cables. These cables carry over 95% of the world's data traffic, making their security a top priority (Brenner, 2024). The average age of European submarine cable systems is 18 years (Rolofs, 2022). The exponentially growing demand for data traffic, due to the AI boom, leads to the concern that older cables may not be able to handle this amount of data (Rolofs, 2022). Installing and maintaining them is increasingly costly; that is why many operators find it more economically attractive to lay new cables than to prioritise repairs, leading to significant waiting times for maintenance (one to three years) (Benner, 2024).

The EU's digital future is increasingly dependent on stable energy production, posing another critical structural challenge (European Commission, 2025e).

The EU's power grid mostly dates back to the last century, with half of its lines over 40 years old, requiring hundreds of billions of Euros in investment to cope with rising green energy output and booming demand from data centres and electric vehicles (Chestney, 2025) (See Figure 5). Connecting new data centres to the grid in current main hubs can take 7-10 years on average, with some projects facing delays of up to 13 years (Forrest, 2025). This could lead to a geographical shift in investment as developers prioritise regions with better access to power, potentially impacting current hubs like Frankfurt, London, Amsterdam, Paris and Dublin, with up to half of Europe's data centre capacity potentially located elsewhere by 2035 (Forrest, 2025).

**Figure 5: The age of different parts of the energy grid. (IEA, 2023, p.27)**




Andreas Schweinar (2025) addressed another problem in an interview. Not only are data centres used from early on until the end of their useful life, but in general, *"all the companies and public authorities are using very old software tools. And now they have the problem, if they want to shift to a new data centre or to a new cloud-based data centre with high software standards, they have to change at first their software level."* This is an extremely time-consuming and costly undertaking.

## Capacity gaps

A critical capacity gap is the shortage of digital skills across the EU. Only 55.6% of adults in the EU had at least basic digital skills in 2023, and at the current pace, the EU is expected to fall significantly short of its 80% target by 2030 (Güell, 2023) (European Commission, 2025c) (See Figure 6). There is also a persistent shortage of ICT specialists, with the EU only halfway to its 2030 target of 20 million employed ICT specialists (Güell, 2023). This shortage is particularly acute in high-demand areas like AI and cybersecurity (European Commission, 2025c). The EU also needs an additional workforce of 299,000 cybersecurity professionals (European Commission, 2025c).

While European organisations excel in scientific publications, they struggle to translate this knowledge into patented innovation, filing fewer patents compared to the US and China (European

**Figure 6: Digital Skills in Europe, compared to the 2023 target. (European Commission, 2025d)**

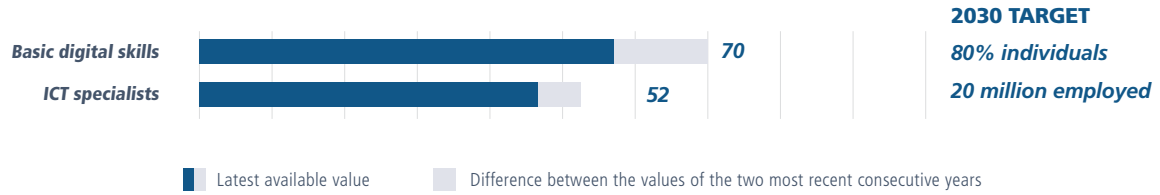
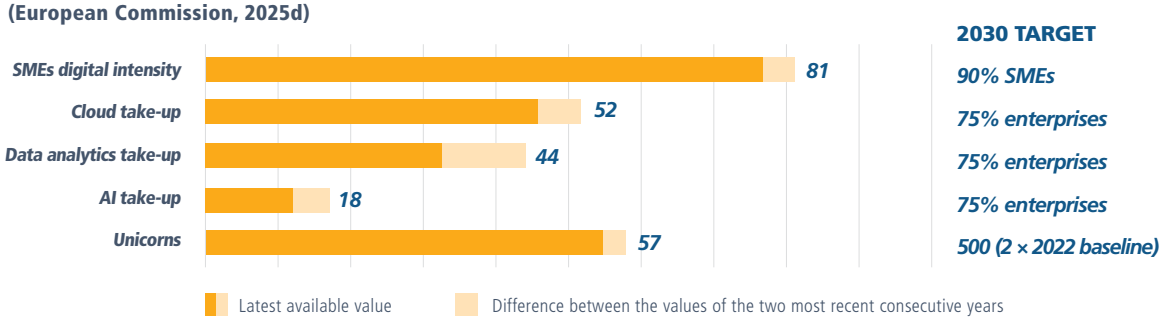



**Figure 7: Digital Transformation of Businesses in Europe, Compared to the 2023 target. (European Commission, 2025d)**




Commission, 2025c). The number of unicorns (a privately held startup that achieves a valuation of over $1 billion) established in the EU rose by 12 units in 2024, reaching 286, but this is a slowdown compared to previous years, and the target of 500 unicorns is not expected to be reached until 2034 without further action (see Figure 7). This is significantly behind China (397) and the US (1687) (European Commission, 2025c).

## OPERATIONAL CHALLENGES

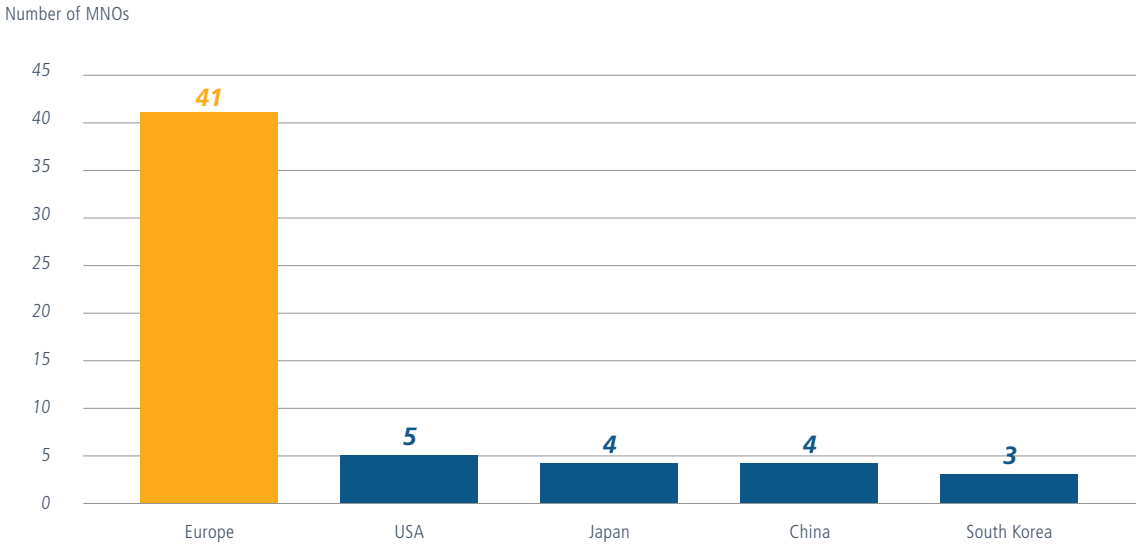
### Inefficiencies

A primary operational challenge for the European ICT sector is its significant market fragmentation (Delgado, 2025). Europe currently has 41 mobile network operators (MNOs) with over 500,000 connections, a big contrast to just 5 in the USA or 4 in China and Japan (Delgado, 2025) (see Figure 8). This fragmented market, coupled with heavy rules and a lack of scalability, has led to a halt in investment growth for the first time in years within the telecom sector.

Beyond telecommunications, Europe's digital innovation ecosystem suffers from a *"fragmented ecosystem with limited specialisation"* (European Commission, 2025c, p.2). Despite its vast economic potential, the Digital Single Market remains fragmented due to a complex landscape of national regulations, administrative procedures and obstacles to data and knowledge sharing, leaving much potential untapped (European Commission, 2025c). This fragmentation also limits the ability of companies, particularly startups, to scale up (Saulnier, 2025).

Compounding this, complex regulations and administrative burdens impose substantial costs and

**Figure 8: Number of MNOs with over 500.000 connections in Europe, China, Japan, South Korea and the USA, 2Q 2024. (Connect Europe, 2025, p. 142)**



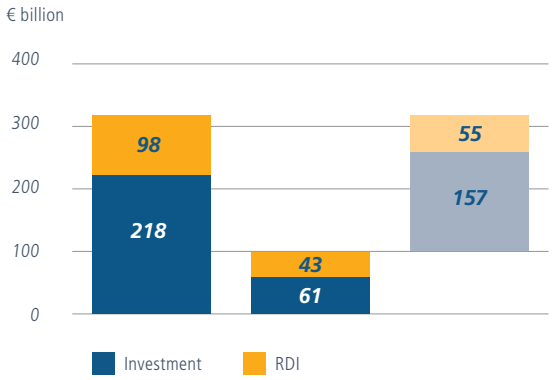

delays on businesses. More than half of European SMEs identify regulatory and administrative obstacles as their greatest challenge (European Commission, 2025c). The EU's digital regulatory framework includes nearly 100 tech-focused laws, comprising thousands of pages, provisions and restrictions, which are often described as *"clumsy and overly heavy-handed"* (Guinea, 2025, p.18), increasing costs and unpredictability for businesses. The additional problem is that ICT evolves at a faster pace than that of the EU decision-making process, consequently parts of the Union's legislative framework quickly become obsolete and their updating takes too long.

## Underfunding

Europe faces a critical challenge of insufficient investment across its ICT sector, particularly when compared to global competitors. Despite European telecom operators investing approximately €58 billion in 2023, this level falls short of ensuring per capita funding comparable to other regions (Delgado, 2025).

Europe's telecom investment per capita in 2023 (€117.9) is almost half that of the USA (€226.4) (Delgado, 2025). To meet its 2030 digital targets, the EU needs an additional €157 billion in annual investment, requiring a total of €316 billion in high-tech digital innovation per year (Saulnier, 2025) (see Figure 9). For context, the combined annual AI investment of the four largest US tech firms (around €200 billion in 2024) already exceeds the EU's entire annual budget (€170 billion per year) (Saulnier, 2025).

**Figure 9: EU investments needs per year. (Janvová et al., 2025)**




The EU's digital innovation efforts are hampered by a limited scale of investment in research and development (R&D) and an insufficient focus on breakthrough innovation (European Commission, 2025c). The US dominates digital R&D, accounting for around 40% of all digital companies and 53% of total R&D investment among those identified in 2023 (European Commission, 2025c).

However, Europe needs not only investment in general, but also long-term investment for the next 30 years, rather than just for the next three years, as Andrew Pidgeon (2025) points out in an interview. Even though people want to see short-term results and don't want to wait 20 years, this long-term investment is important to properly expand the infrastructure.

The lack of private capital for "big ticket" investments within the EU also forces many European startups to seek late-stage growth capital from external venture capital funds, often resulting in them relocating their corporate headquarters outside the EU (European Commission, 2025c).

In quantum computing, the EU struggles to mobilise private finance, attracting only 5% of global private funding, while 50% goes to US companies (European Commission, 2025c). The investment needs for developing cloud infrastructures are "massive" (European Commission, 2025c, p.8). The top 11 countries make up 90% of the patents granted globally, with Germany, France, Italy and the Netherlands contributing 27% (Soller, 2025).

**The quantum communication market is projected to reach $11 billion to $15 billion by 2035.**

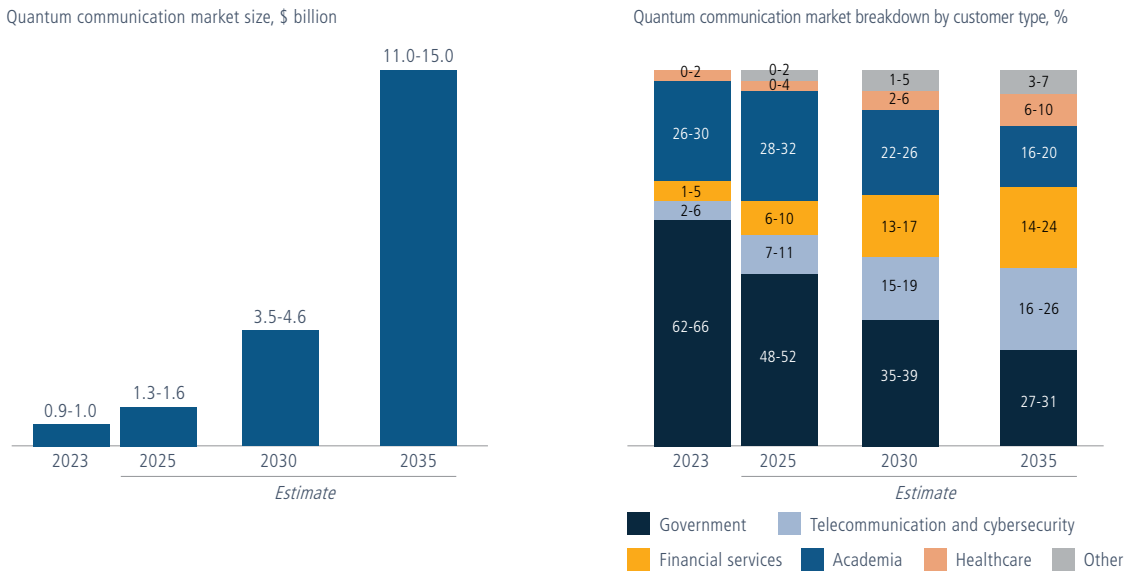
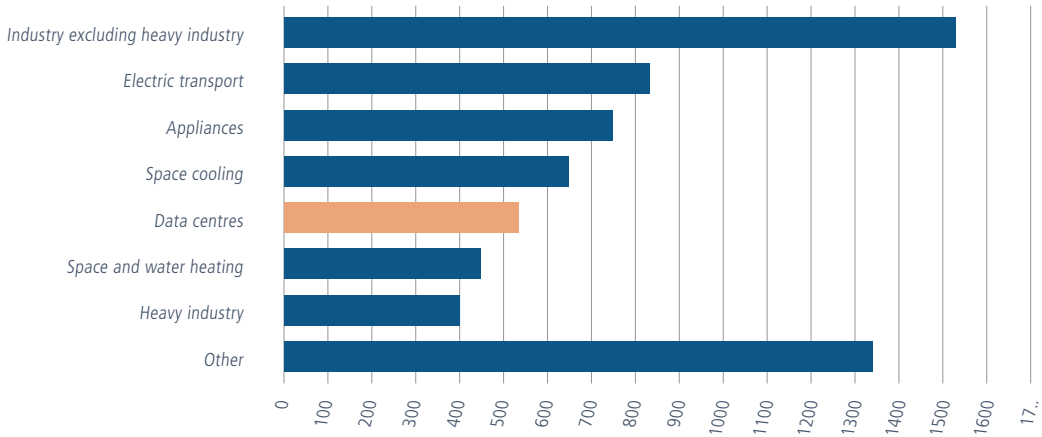


**Figure 10: Increase in electricity demand by sector, 2024-2030. (IEA, 2025)**




## CROSS SECTOR DEPENDENCIES – INTERDEPENDENCIES WITH OTHER CRITICAL INFRASTRUCTURE

### ICT and Energy

The relationship between the ICT sector and the energy sector is characterised by a dual dependency: ICT's significant demand for energy and the energy sector's increasing reliance on ICT for efficient construction and operation, including maintenance.

Firstly, the ICT sector cannot survive without the energy sector, as it is virtually entirely dependent on it. Secondly, the digital sector, encompassing AI, high-performance computing and edge networks, is experiencing exponentially rising energy demands (European Commission, 2025c). This discrepancy poses a significant barrier to scaling key digital technologies and fully leveraging AI and data-driven innovation for economic competitiveness (European Commission, 2025e).

Data centres in particular require substantial amounts of electricity, a challenge exacerbated by the rapid deployment of AI accelerators and dense computing clusters (European Commission, 2025c) (See Figure 10).

To address these issues, efforts are underway to reduce the energy consumption of digital services, focusing on energy-efficient semiconductors and climate-neutral edge nodes (Bijlagen bij COM, 2024).

Conversely, the energy sector, particularly the power grid, relies heavily on ICT networks for monitoring, control and performance optimisation (Ahmed, 2019). Most critical infrastructures, including energy, are controlled and monitored by Industrial Control Systems (ICSs), with ICS-Supervisory Control and Data Acquisition (SCADA) being a fundamental component of European critical infrastructures (Markopoulou & Papakonstantinou, 2022). Increased reliance on ICT is seen as crucial for improving the power grid's resilience through technologies like phasor measurement units for wide area monitoring and bi-directional communication for active distribution networks (Ahmed, 2019). ICT also helps stabilise the grids via the smart grids systems, especially when dealing with energy fluctuations.

The energy production segment is also increasingly reliant on ICT systems, starting from the design and construction of the production facilities. The complexity of these facilities, together with their safety and security (and thus resilience) requirements, have increased over the years, therefore engineers need ever complex ICT systems to deliver such projects. Furthermore, ICT has become essential in enabling all aspects of energy production: daily operations, maintenance, supervision, safety & security, market connectivity and transactions, training, etc. The use of ICT is even more important in the case of renewables, due to their intermittence and often decentralised structure.

ICT also has a role to play in energy storage, from building the facilities to their operations, in connection to energy production, grid availability and market demands. Safety and security measures for these facilities also incorporate ICT systems.

While discussions on energy topics are generally focused on the larger system segments and players, the use of renewables, particularly solar power, has led to a significant decentralisation of the production capacities at local and even individual level (the prosumers). In addition to the technological advancements in solar panels, batteries, electric vehicles and similar technologies, this decentralisation would not have been possible without the use of the ICT systems and infrastructure. Consequently, the resilience of ICT (and energy) infrastructure can be very directly linked to the individual level.

## ICT and Water

As the digital economy expands, particularly with the proliferation of AI, this dependency is becoming an increasingly pressing concern (see Figure 11).

**Figure 11: Share of energy-related water consumption in annual total water consumption for data usage (%). (Farfan, Lohrmann, 2023)**

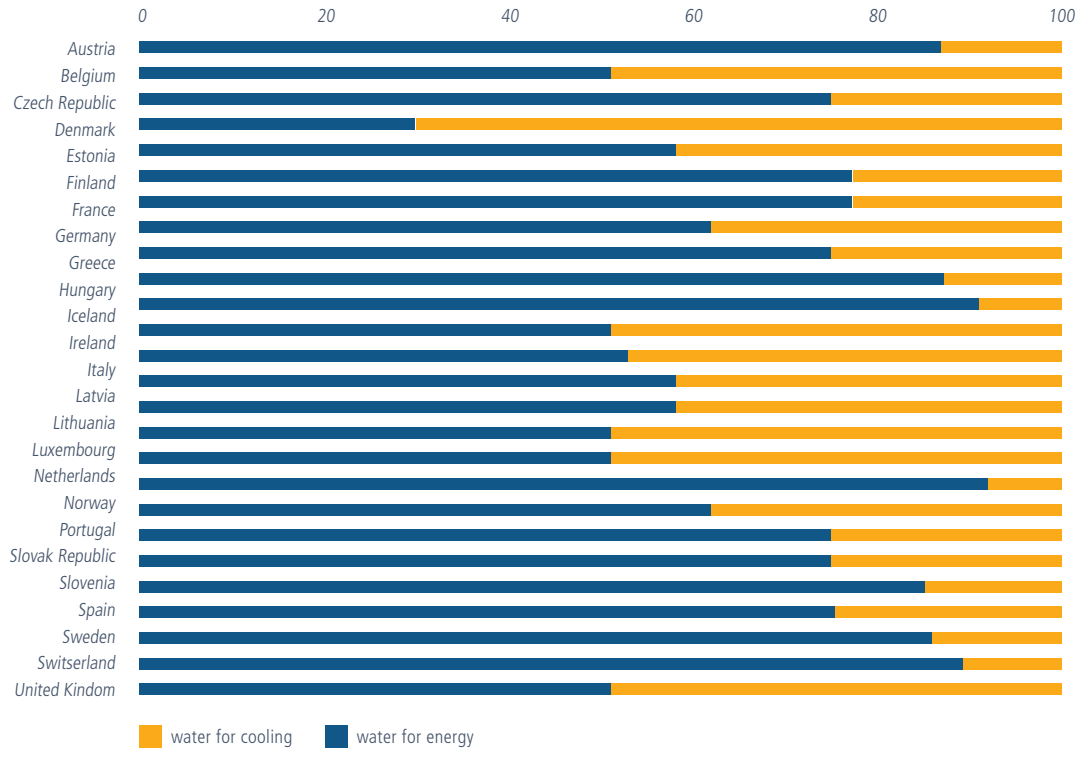
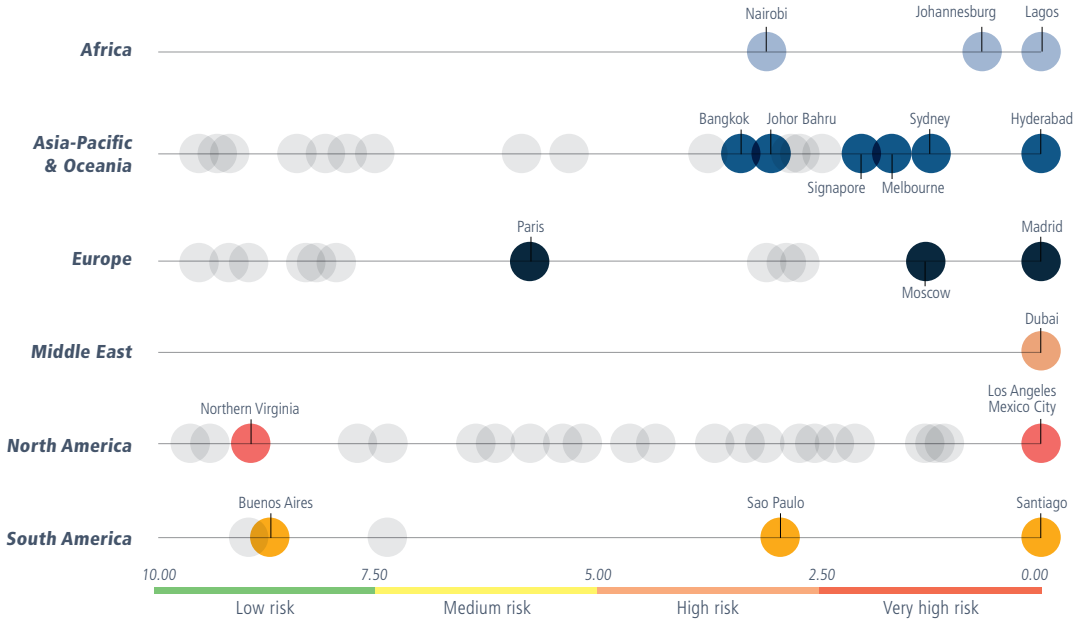


**Figure 12: Distribution of 100 data hub cities on our Water Stress 2050 SSP585 Index. (May, Schwartz, 2025)**




Data centres, the physical backbone of the digital world, are inherently power-intensive and generate significant heat, necessitating robust cooling systems to maintain stable operation (Vertiv, 2025). This cooling process, in turn, can be highly water-intensive (European Commission, 2025c). For context, a single data centre operating at full capacity might consume 16 million gallons (approximately 60,000 cubic meters) of water annually. To put this into perspective, 1 million gallons of water can support 20 EU households for a year (Breukel, 2025).

The surge in demand for high-performance computing, driven by AI workloads like generative AI training and inference, exacerbates this challenge, as these dense computing clusters generate even more heat and require substantial electricity and water for cooling (European Commission, 2025c).

Studies project that by 2027, global AI demand alone could consume between 4.2 and 6.6 billion cubic meters of water a year (European Commission, 2025c). By 2030, 52% of global data centre hubs will be exposed to high or very high water stress, rising to 58% by 2050, which is also having a significant impact on parts of Europe (May & Schwartz, 2025) (See Figure 12).

However, ICT systems can also bring significant benefits, by reducing water consumption and pollution via improved industrial and agricultural practices, technologies and infrastructure (new or modernised), as well as by ensuring their (cyber) security. The same principles apply to sanitation systems that serve both urban and rural areas.

## ICT and Transport

The transport sector is another critical European infrastructure that relies heavily on ICT, from the design and building of infrastructure and vehicles to managing traffic and logistics or enabling modern e-mobility solutions.

The investments in transport infrastructure are often not just the largest but also the costliest when compared to other infrastructure types. They often require highly complex solutions due to increased urbanisation, geographical aspects, legacy systems to be integrated, the use of new technologies but also the links to other infrastructure, particularly energy and ICT. To deliver transport infrastructure projects, the use of ICT systems such as Building Information Modelling (BIM), AI and Big Data by engineers is becoming 'business as usual'. Moreover, the operation, supervision and maintenance of transport infrastructure is increasingly dependent on ICT.

Traffic in all transport modes is also heavily reliant on ICT-based solutions, and this includes both wayside/infrastructure and on-board systems. Their complexity will only increase with the automation of operations.

Furthermore, there are other systems that function within or near to transport infrastructure and operation systems, at various levels of connection (e.g. ticketing, passenger information systems, etc.). This not only further increases the complexity of systems and of the 'systems of systems' but also requires additional capacity in terms of ICT infrastructure.

Change is generally gradual, due to the nature of the sector, but there are active efforts to decouple cybersecurity needs from the otherwise lengthy procedures of some transport segments, e.g. railways, thus improving resilience.

The ongoing digital transformation, marked by ICT-based solutions and the convergence of IT and operational technology (OT), has significantly increased the transport sector's cyber risk profile. It was the second most targeted sector for cyber incidents in the EU in 2024 (ENISA A) and the trend continued in 2025.

Lastly, the rising adoption of e-mobility, including electric vehicles (EVs) and electric railway systems, increases the interdependencies between the power grid, ICT and transportation networks (Ahmed, 2019). For instance, a failure in a subway passenger station can lead to traffic congestion and increased charging demand for EVs and electric buses. Conversely, a lack of available EV charging stations can significantly increase demand on the subway system (Ahmed, 2019).

# Analysis of geopolitical and climate threats

## GEOPOLITICAL RISKS

### Supply Chain Vulnerabilities

The security of ICT supply chains has become a paramount concern, largely due to their complexity, wide reach and the significant cascading effects that can result from a compromise (ENISA B, 2024). Supply chain compromise of software dependencies is predicted to be the most prominent cyber threat in 2030, according to ENISA, despite a slight decline in its overall impact and likelihood score compared to previous years (ENISA C, 2024) (See Figure 13). This vulnerability arises because *"more integrated components and services from third-party suppliers and partners could lead to novel and unforeseen vulnerabilities with compromises on the supplier and customer side"* (ENISA D, 2024, p. 2).

Threat actors, from nation-states to cybercriminals, exploit these vulnerabilities to conduct sabotage, theft and network reconnaissance, and inject malicious code into commodity software (NIS Cooperation Group, 2023). Recent incidents, such as the critical XZ Utils backdoor discovered in March 2024, highlight how malicious actors can gain access

**Figure 13: New prioritisation of threats. (ENISA (F), 2024, p. 7)**

| Threat | Impact * Likehood | Impact | Likehood |
|---|---|---|---|
| Supply Chain Compromise of Software Dependencies | 17,71 | 4,21 | 4,21 |
| Skill Shortage | 17,20 | 4,10 | 4,20 |
| Human Error and Exploited Legacy Systems within Cyber-Physical Ecosystems | 16,69 | 3,96 | 4,22 |
| Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem [Optional] | 16,21 | 4,05 | 4,00 |
| Rise of Digital Surveillance Authoritarianism / Loss of Privacy | 15,34 | 3,96 | 3,88 |
| Cross-border ICT Service Providers as Single Point of Failure | 15,12 | 4,14 | 3,65 |
| Advanced Disinformation / Influence Operations (IO) Campaigns | 14,38 | 3,42 | 4,21 |
| Rise of Advanced Hybrid Threats | 14,03 | 3,68 | 3,81 |
| Abuse of AI | 13,22 | 3,43 | 3,86 |
| Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure [Optional] | 12,99 | 3,68 | 3,53 |
| Lack of Analysis and Control of Space-based Infrastructure and Objects | 12,52 | 3,63 | 3,45 |
| Targeted Attacks (e.g. Ransomware) Enhanced by Smart Device Data | 12,29 | 3,39 | 3,63 |
| Increased Digital Currency-enabled Cybercrime [Optional] | 10,25 | 3,06 | 3,35 |
| Manipulation of Systems Necessary for Emergency Response [Optional] | 10,02 | 3,27 | 3,07 |
| Tampering with Deepfake Verification Software Supply Chain [Optional] | 9,83 | 3,00 | 3,28 |
| AI Disrupting/Enhancing Cyber Attacks [Optional] | 9,78 | 3,07 | 3,19 |
| Malware Insertion to Disrupt Food Production Supply Chain [Optional] | 9,33 | 3,11 | 3,00 |
| Exploitation of E-health (and Genetic) Data [Optional] | 9,32 | 3,11 | 3,00 |
| Attacks Using Quantum Computing [Optional] | 7,32 | 2,76 | 2,65 |
| Disruptions in Public Blockchains [Optional] | 5,96 | 2,47 | 2,41 |
| Technological Incompatibility of Blockchain Technologies [Optional] | 5,91 | 2,25 | 2,63 |

by becoming project maintainers through social engineering campaigns (ENISA E, 2024).

Submarine cables can be seen as a part of the supply chain. Geopolitical tensions further exacerbate the risk, with state-sponsored malicious activity targeting these cables likely to increase (Insikt Group, 2025). Concentrating cables along similar routes or at single cable landing stations increases systemic risk, making multiple cables vulnerable to sabotage or espionage (Insikt Group, 2025).

The most recent example of such supply chain vulnerabilities comes from the transport sector, with the Norwegian public transport operator Ruter discovering that its electric buses made by the Chinese company Yutong Group could be remotely accessed by the manufacturer and even turned off (Euronews, 2025). While the details were still being clarified at the time this report was being written, the discovery shows the extent to which ICT systems and infrastructure are interconnected, and the potential cascading effects that one security or safety incident may trigger. The discussion also relates to the increased European dependence on non-EU states and the growing cybersecurity threats from state and non-state actors alike, which are discussed in the following two subchapters.

### Strategic Dependence on Non-EU States

Europe faces a growing digital dependency on foreign powers, particularly the United States and, increasingly, China, which poses a direct threat to its sovereignty and economic competitiveness (Silicon Saxony, 2025).

Approximately 70% of cloud capacity in Europe and 85% of Graphics Processing Units (GPUs) essential for AI are currently controlled by US providers like Amazon Web Services (AWS), Microsoft and Google (Silicon Saxony, 2025). Meanwhile, the market share of European providers continues to decline (see Figure 14). That was also an aspect in the interview with Andreas Bach (2025), who mentioned: *"We don't have a similar play in Europe now, on the same level that can compete with them. From a political aspect and also from an economic aspect, that's kind of a risk."*

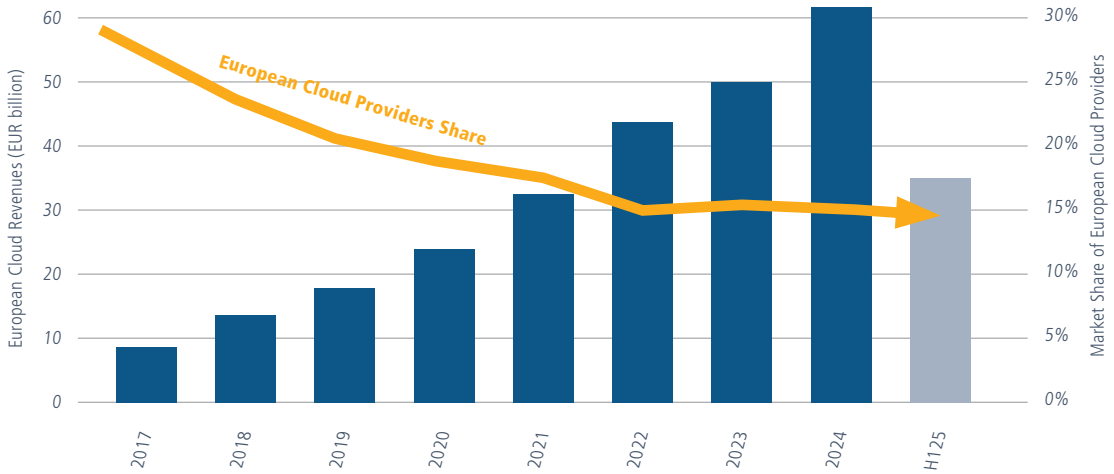
Moreover, as noted by several EFCA member companies, some of the ICT systems are so interconnected that the data sets of the major IT companies in the USA are now de facto part of Europe's critical ICT infrastructure. The AI systems in particular will not function effectively without the US datasets.

This reliance creates significant vulnerability to potential digital tariffs or service disruptions, as seen in the ongoing tariff disputes between Europe and the US (Silicon Saxony, 2025). A complete withdrawal of US hyperscalers would create a massive gap in IT connection capacity and data storage (about 40 exabytes for storage), which European providers cannot compensate for in the short or medium term (Silicon Saxony, 2025).

Consequently, at European level there is currently a rise in the demands towards EU and national officials to develop a sovereign cloud(s). In addition to mitigating part of this strategic dependence on non-EU states, these initiatives often involve collaboration between cloud providers, local governments and industry partners, which can lead to new partnerships and business models, expanding opportunities for innovation and growth.

The second area is semiconductors. The EU's share of global value chain revenues for semiconductors was 10.5% in 2024, far from the 2030 target of 20%, with huge investments accelerating in other regions, especially the US and China (European Commission, 2025c).

**Figure 14: European Cloud Provider Share of Local Market Through the Years. (RENO, 2025)**




As already mentioned above, non-European private operators, including US tech giants (Google, Amazon, Meta, Microsoft) and Chinese companies (Huawei), now control over half of the undersea cable bandwidth, raising concerns about Europe losing its competence and sovereignty in this critical area (Leitzcloud, 2022). Furthermore, the concern about espionage and sabotage is rising. This was seen in the recent incidents connected to geopolitical tensions in the Baltic Sea, involving Russia, or the possibility that China was building undersea cables in Marseille, leading to fears of data interception (Insikt group, 2025), (Leitzcloud, 2022).

## Cybersecurity

Disruptive digital attacks in various EU countries have recently increased significantly. For instance, these types of attack in Greece doubled over the course of only a few months, with many attributed to Russian-backed groups, and are specifically targeting election-related services (Gatopoulos, 2024). Another, very recent example is the cyberattack in September 2025 against airports in several large European cities (e.g. Brussels, Berlin, London), which heavily disrupted the air traffic (Reuters, 2025). It is important to note that the attack did not concern any elements of the air transport itself, but one of the ICT services that, from a technical point of view, is not connected to them: the check-in systems. However, the actual impact of this cyberattack shows the high degree of operational interconnection between the ICT systems in the transport sector, and the cascading effects that any component of this ecosystem may trigger when a security breach or any other failure occurs.

These attacks involve on the one hand, threat actors and attack types. State-nexus actors (e.g., Russia-nexus and China-nexus groups) continue to be prominent, engaging in continuous cyberespionage campaigns against EU member states and institutions (ENISA B, 2024). They

employ sophisticated techniques like "Living Off the Land" and remote monitoring software to avoid detection (ENISA E, 2024).

Hacktivist activity is also increasing and becoming more unpredictable, often using tactics like distributed denial of service (DDoS) attacks and website defacements, especially in response to geopolitical conflicts (ENISA B, 2024). Ukraine was the primary target for hacktivism in Europe, experiencing 16.9% of attacks, due to the war with Russia (see Figure 15) (All about security, 2025). In the cybercrime ecosystem, ransomware remains one of the most impactful threats, with a shift from encryption to data exfiltration and the double extortion tactic becoming the norm (ENISA B, 2024).

### Physical Threats

An example of how a geopolitical threat can further weaken a vulnerability in Europe's ICT infrastructure can be seen in the case of submarine cables.

As described above, one weakness of the infrastructure is the ageing submarine cables used for internet connections. In addition to their age, there is also the fact that they are often no thicker than a garden hose on the seabed and remain physically vulnerable (Voce et al., 2025).

Geopolitical uncertainties and conflicts have turned submarine cable infrastructure into a "flashpoint" (Chee, 2024). European governments are increasingly concerned, with officials, including defence ministers from Germany and Finland, naming hostile actors, such as Russia, as the likely cause of these incidents (Voce et al., 2025).

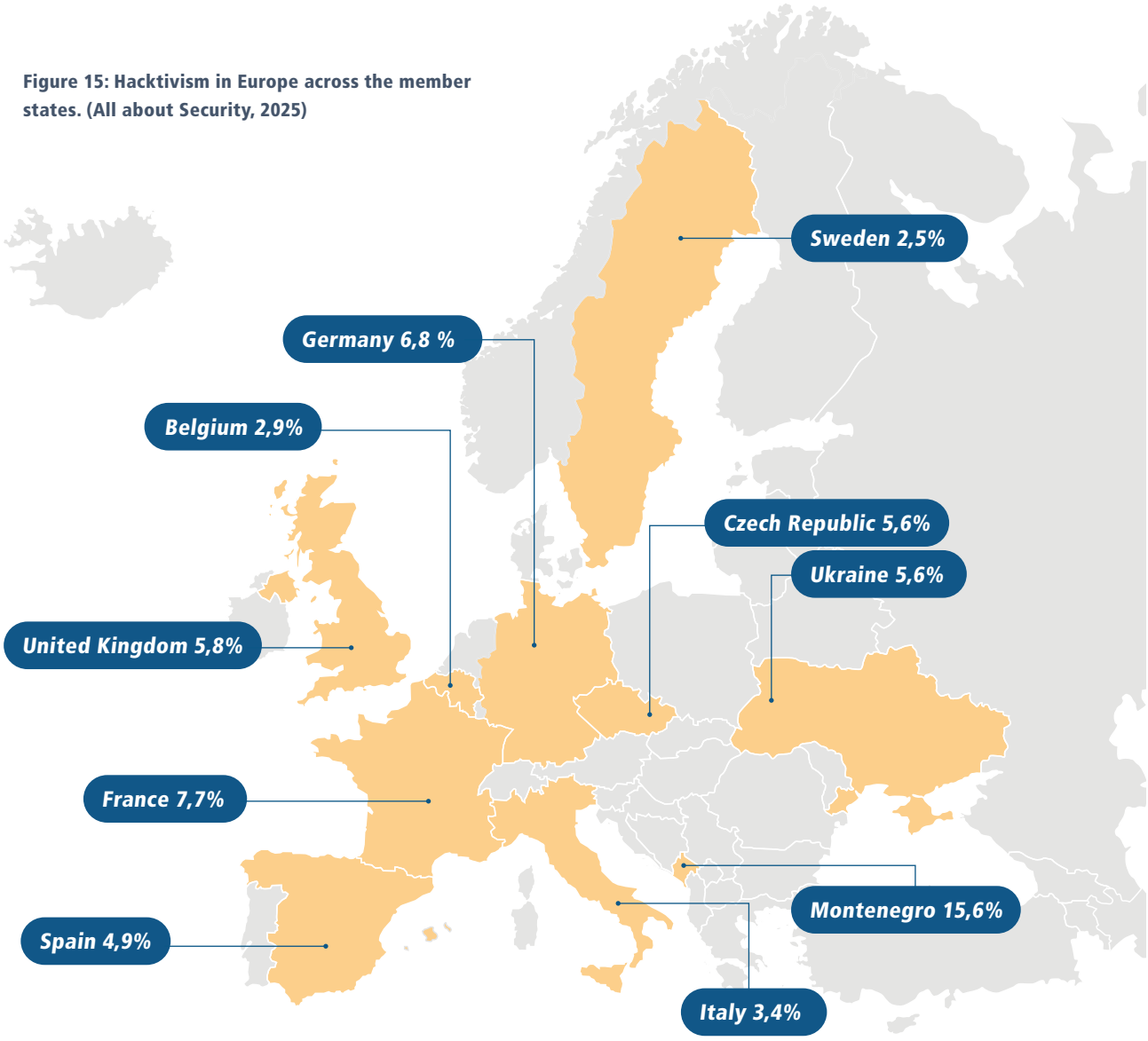



**Figure 15: Hacktivism in Europe across the member states. (All about Security, 2025)**

Experts also express concerns about "hybrid warfare," which involves deniable actions by other nations designed to cause disruption without escalating to an attributable act of war (Aitken, 2025). Additionally, policies for decommissioning legacy equipment and networks are now motivated by security concerns, as older systems can retain vulnerabilities that malicious actors might exploit. This implies that older segments of the network, if not properly upgraded or replaced, could be more susceptible in a heightened threat environment (Feasey et al., 2024).

A prominent recent example of this vulnerability and the impact of geopolitical tensions occurred on Christmas Day 2024, when Finland began investigating a mysterious incident that severed

undersea cables connecting the country with Estonia (Voce et al., 2025). Finnish authorities could not rule out sabotage, and the following day, they seized the cargo ship "Eagle S," registered in the Cook Islands and owned by a UAE company, which was carrying Russian oil (Voce et al., 2025). This vessel is suspected of being part of a "shadow fleet" of ageing tankers used to evade sanctions on Russian oil. Finnish authorities suspect the "Eagle S" damaged three fibre-optic connections with Estonia and one with Germany. This incident is part of a series of suspicious outages affecting undersea energy pipelines, telecommunication cables, and power connections in the Baltic Sea, putting European countries on high alert (Voce et al., 2025). Estonia's Foreign Minister, Margus Tsahkna, stated that the damage to subsea installations has become so frequent that it is difficult to believe it is merely accidental, asserting that such damage must be regarded as *"attacks against our vital structures"* (Lehto & Sytas, 2024).

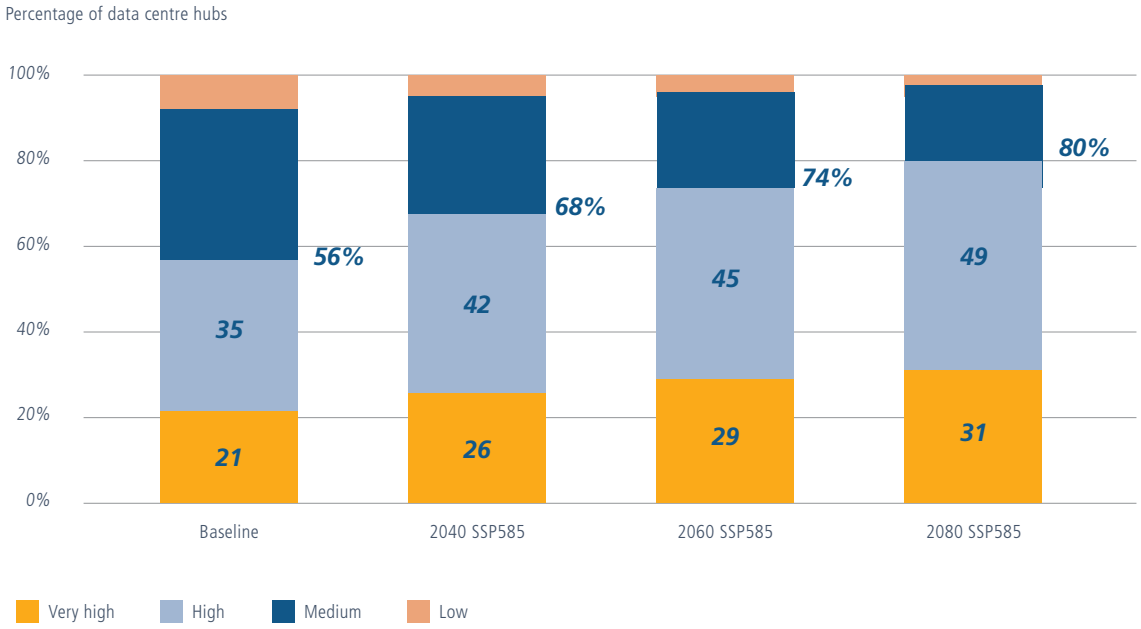
## CLIMATE CHANGE IMPACTS

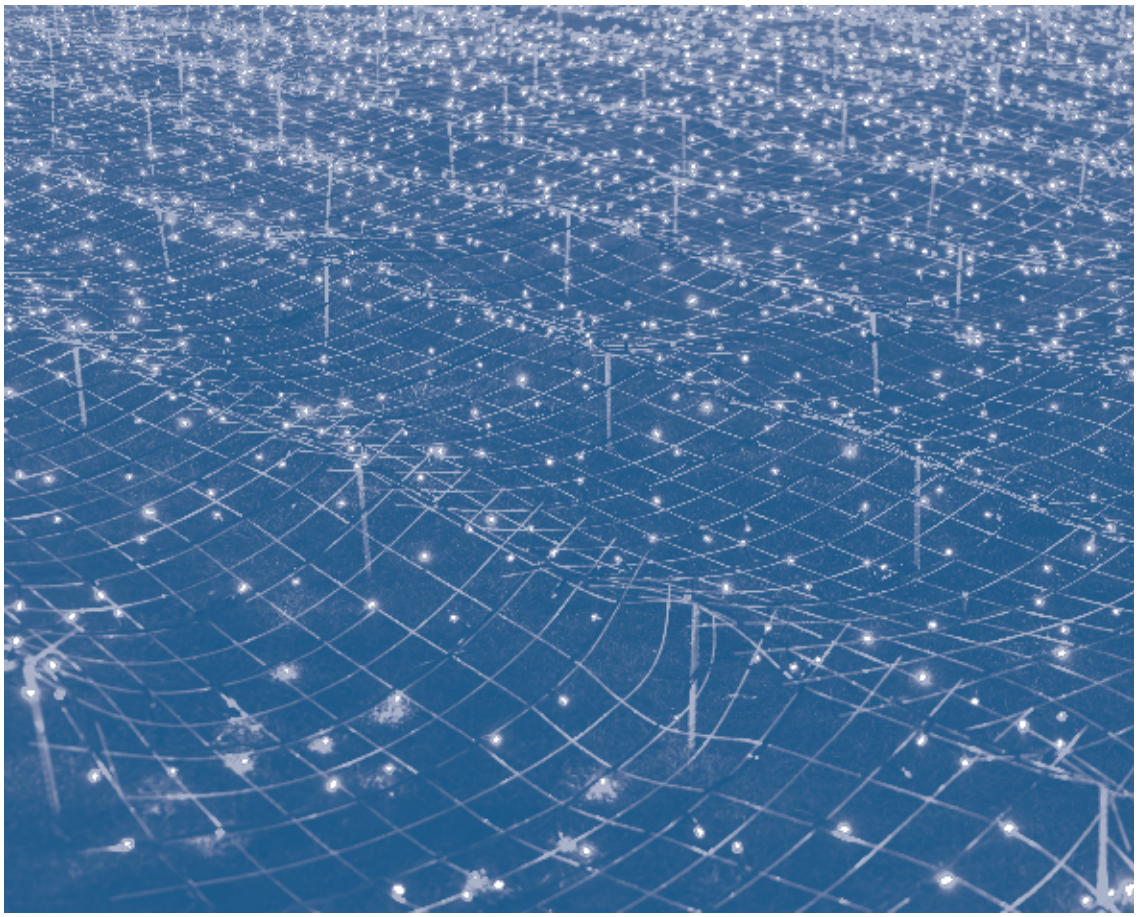
Europe experienced its warmest temperatures and most widespread flooding since 2013 in 2024, making climate change impacts a threat to ICT infrastructure (Antonio et al., 2023).

One area of the ICT sector that is particularly vulnerable to climate change and its consequences is data centres (Voice&Data, 2024).

Rising temperatures and heatwaves lead to an increased demand for cooling, which drives up operating costs and energy consumption for

**Figure 16: Distribution of 100 data hub cities on our cooling degree days scenario indices over time. (May, Schwartz, 2025)**





data centres. Over half of the world's 100 largest data centre hubs are already exposed to high or very high heat-related risks (May & Schwartz, 2025). By 2040, this proportion is projected to rise to 68% under a high emissions scenario and to 80% by 2080 (May & Schwartz, 2025). The average increase in cooling demand is expected to be 83% between 2030 and 2080 (May & Schwartz, 2025). (See Figure 16).

The danger here is that overheating servers can lead to system failures. One example of this is that in June 2025, the Google Cloud region Europe-West (Milan) went offline for 90 minutes because AI-intensive racks were shut down due to automatic thermal shutdowns. Oracle's Frankfurt region also experienced latency spikes of 170%, triggered by the saturation of HVAC systems in modular cooling bays (Agostini, 2025).

Telecommunications infrastructure worldwide is threatened by extreme heatwaves, droughts and wildfires, impacting productivity and increasing infrastructure damage (Voice&Data, 2024). Metals in cables can deform, expand and sag in extreme heat, and batteries are affected by power leaks.

Internet infrastructure e.g., submarine cables, suffers from climate change too. These cables are extremely vulnerable to damage from natural events like marine earthquakes, storms or corrosion (Blenker, 2024).

# Best Practice and Lessons Learned

## CASE STUDIES: SUCCESSFUL RESILIENCE INITIATIVES

### Spain's Cybersecurity Operations Centre (COCS)

Spain's COCS and its National Network of SOCs provide a coordinated response to cyber incidents, centralising security event management (SIEM), proactively hunting threats, and improving information exchange between public and private SOCs to enhance prevention, protection, detection, and response capabilities (Gobierno de Espana, n.d.). These efforts are crucial given that over 100,000 cyberattacks were detected in Spain in 2024, with one considered very serious every three days, and cyberattacks having increased by 300% since 2015 (Ministerio Para la Transformación digital y de la función pública, 2025). Although this is not a new approach to ensuring greater cybersecurity, Spain clearly stands out by exceeding the average in European countries. Spain's commitment is reflected in its standing as the second country globally, behind the United States, in the number of cybersecurity centres. (Ministerio para la Transformación Digital y de la Función Pública, 2025).

### The NIST Cyber-Resiliency Framework (United States)

The US National Institute of Standards and Technology (NIST) has developed a comprehensive Cyber-Resiliency Framework, outlined in publications such as NIST Special Publication 800-160 Volume 2. This framework provides a flexible, systems-engineering-based approach to help organisations build IT systems that can anticipate, withstand, recover from and adapt to cyberattacks, particularly focusing on advanced persistent threats (APTs) (Ross et al., 2019). It emphasises developing *"trustworthy, secure IT components, services, and systems that are cyber resilient"* to ensure that systems can continue to operate even in a degraded or debilitated state while carrying out mission-essential functions (Ross et al., 2019). The framework extends its focus to operational technology and industrial control systems, allowing organisations to apply cyber-resiliency approaches and controls to counter adversarial attacks in these critical sectors (Edge Editors, 2021). The NIST framework defines clear cyber resiliency goals: Anticipate, Withstand, Recover and Adapt (Ross et al., 2019).

# Recommendations

## RECOMMENDATIONS FOR CONSULTING ENGINEERS

The following shows a selected set of recommendations, based on the prior analysis.

### Adopt Integrated and Preventive Approaches

Consulting engineers should shift from reactive to preventive resilience strategies. This requires adopting an integrated cyber-physical perspective that combines cyber and physical risk analysis and accounts for cascading effects across interconnected infrastructures (European Commission, 2025c). Climate and man-made threats must be addressed in an integrated manner, sometimes reaching a balance between the various requirements, to achieve the resilience goal. At the same time, they must critically reflect on traditional methods and continuously update their skills. As Pierluigi Bassetto (2025) emphasises, older approaches are no longer sufficient in a world shaped by climate change and geopolitical shifts. Engineers should instead become pioneers of new methods, focusing on a few key aspects to monitor and address effectively, while avoiding an overreliance on complex technologies that waste resources. Building networks of proposals and solutions, supported by continuous training and knowledge exchange, is essential for long-term resilience.

### Embed (Cyber) Resilience into System Design

(Cyber)Security should not be an afterthought added to systems late in their lifecycle. Instead, engineers must embed resilience principles at the design stage ('resilience by design'), applying constructs such as goals, objectives, techniques and design principles consistently across system development, upgrades, and repurposing (Ross et al., 2019). This implies integrating safeguards from the outset and making resilience a core design parameter, regardless of system size or complexity. Consulting engineers should also be prepared to make careful trade-off decisions when selecting techniques, since no single measure (e.g., redundancy, segmentation, deception or diversity) is universally optimal.

### Harness Data and Monitoring for Adaptive Responses

Resilient systems must include advanced, data-driven monitoring capabilities. Engineers should leverage techniques such as sensor fusion, contextual awareness and analytics to detect anomalies in real time, assess potential impacts, and trigger adaptive responses (Ross et al., 2019). This shift from static defence to dynamic resilience requires not only technology but also methodological expertise in combining data streams, interpreting them and building feedback loops for decision-makers.

## RECOMMENDATIONS FOR POLICYMAKERS

### Create a Supportive Regulatory and Investment Environment

Policymakers should aim to reduce regulatory fragmentation and over-regulation in Europe's digital economy. This means conducting a systematic review of current digital legislation to ensure that both public and consumer protection is preserved while competitiveness is strengthened (Guinea & Sharam, 2025). At the same time, governments need to address Europe's chronic R&D gap in ICT by providing stronger incentives for private companies to invest in frontier technologies. Political leaders must also take greater ownership of resilience decisions, since their allocation of funds can either accelerate or hinder the development of

solutions (Bassetto, 2025). Moreover, there is an urgency to simplify the administrative and regulatory procedures related to permitting, to speed up investments and projects. However, this approach to 'cutting red tape' should not be done to the detriment of quality, environmental protection and resilience for the critical infrastructure and the CEF projects.

### Strengthen EU Cybersecurity and Infrastructure Resilience

A coherent implementation of the EU's evolving cybersecurity framework is critical. This includes effective transposition and enforcement of NIS2, the CER Directive and the Cyber Resilience Act. A harmonisation of this legislation is also necessary, to provide stakeholders with clarity for their investments and operations, avoid overlaps and possibly reduce some of the administrative burden. Here, it is particularly important to have an improved approach to critical resilience entities' protection at EU level, as today this is mostly done by the Member-States, which have very different geographic, economic, political, etc. contexts and priorities. Cooperation should be improved both between the national authorities that oversee critical entities, and between the relevant public and private sector stakeholders. The reason for the latter is that while the security and/or defence national authorities have the final say when it comes to an emergency, it is mostly the civil sector, including the consulting engineers, which are tasked with building and the daily operation of these critical entities and/or services. In parallel, policymakers should scale up support for applied projects that develop innovative tools for protecting critical infrastructure against combined cyber-physical threats (European Commission, 2025c). Coordinated supply-chain security strategies at EU level are equally important to mitigate vulnerabilities introduced by third-party dependence (ENISA B, 2024). National and EU crisis response capacities, such as CSIRTs, should be further equipped with scalable tools and tested through structured cross-border exercises.

### Improving the EU Public Procurement Framework

While public procurement is not part of the EU digital policies, its importance is crucial in the case of the contracting and implementation phases of infrastructure projects. Given the current review of the EU public procurement legislative framework, the new rules should ensure that quality and resilience are properly included in the tendering process via mandatory criteria. Curtailing to the greatest extent the use of the lowest price for intellectual (engineering) services is another recommendation, since quality can seldomly be achieved via the cheapest solutions. Moreover, improved public procurement rules can support the roll-out of new technologies, helping the EU R&I investments and EU producers access the markets. This approach should particularly be applied in the tenders for critical ICT infrastructure and the digital component of the CEF. Strategic purchases that are envisaged via the new public procurement legislation should include high-quality raw materials, equipment, etc. for the performance and resilience of the ICT infrastructure while moving away from the current international dependencies (EFCA Paper on Public Procurement, 2025).

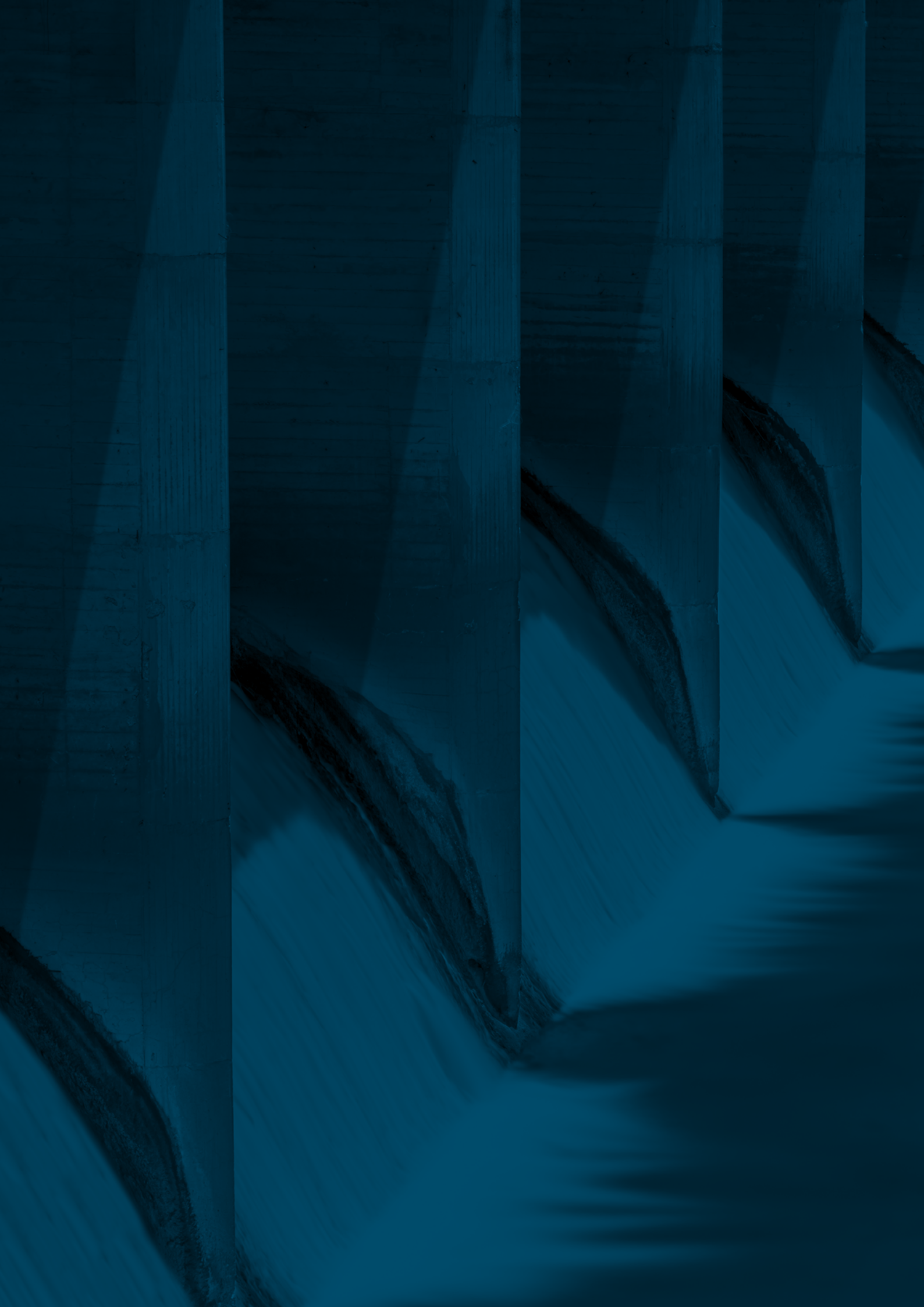
### Standardisation

Further standardisation activities should be sought by the EU institutions and the European companies, especially on data and data exchanges. This can help ensure the EU to retain (some of) sovereignty on both its data and the exchange process. While much of the work can be done directly through the existing European standardisation bodies, CEN-CENELEC and ETSI, this must subsequently be taken at the international level, in standardisation bodies

such as IEC or IEEE. This would ensure not only the dissemination of EU standards but would also reverse the trend of EU dependency on non-EU suppliers.

### Invest in Skills and Human Capital

Resilience cannot be achieved without people. Policymakers should expand national digital skills initiatives and Science, Technology, Engineering, Mathematics and Digital (STEMD) strategies, with a particular focus on improving access in rural areas and increasing the participation of women in ICT professions (Guinea & Sharam, 2025). The development of cybersecurity skills should receive additional attention and support at EU, national and regional levels. A digitally skilled workforce provides the foundation for both innovative ICT development and effective resilience management. Moreover, the need for a digitally skilled workforce should be compounded with skill shortages in other critical sectors, transport being one of the most relevant examples. Investment in human capital ensures that Europe not only develops cutting-edge infrastructure but also has the expertise to protect and adapt it in a volatile global environment.



# Conclusion

The European ICT sector plays a key role in the functioning of all other critical infrastructures and is likely to become even more important as digitalisation progresses.

This is why the confrontation with significant structural, operational, and geopolitical weaknesses is so problematic.

Among these weaknesses, infrastructure, insufficient funding compared to global competitors, and a lack of skilled workers and digital skills stand out. This makes the sector even more vulnerable to external shocks, which are further exacerbated by geopolitical risks such as dependence on third countries and cyberattacks.

Added to this is the strain on the sector's physical infrastructure from the adverse effects of climate change, such as heat, flooding and growing water scarcity.

However, there is already a sound European legal framework, encompassing the Directive on the Resilience of Critical Entities, DORA, NIS2, and the Cyber Resilience Act, which lays important foundations for greater resilience.

Yet to ensure stronger and long-term security, a combination of measures from consulting engineers and political strategies is needed. The latter must encompass improved resilience-related legislation, better public procurement rules, a reduction in the administrative burden, standardisation actions and increased investments in human capital.

The future will depend on whether Europe succeeds in implementing the necessary policies and investments, which will lead to achieving digital sovereignty by expanding its own technological (e.g. cloud and semiconductors) and workforce capacities. Only through an integrative approach can the resilience of the ICT sector be sustainably strengthened and Europe's dependence reduced.

# References


Abhau, Ralf. (2025). *Cloud Dienste aus den USA werden zu einer großen Gefahr für Europa. CSAnet GmbH. Retrieved Aug 15, 2025, from* **https://csanet.de/cloud-dienste-aus-den-usa-werden-zu-einer-grossen-gefahr-fuer-europa/**

Agostini, Martino. (2025). *Europe's heatwaves are breaking data centers – and forcing a rethink of digital infrastructure. Medium. Retrieved Aug 05, 2025, from* **https://medium.com/@tarifabeach/europes-heatwaves-are-breaking-data-centers-and-forcing-a-rethink-of-digital-infrastructure-6bbc36812aee**

Ahmed, Ali A. Mohame d. (2019). *On the Rising Interdependency between the power grid, ICT Network and E-Mobility: Modeling and Analysis. MDPI.*

Aitken, John. (2025). *Undersea Cables are vulnerable to sabotage-but this takes skill and specialist equipment. RAND. Retrieved Aug 05, 2025, from* **https://www.rand.org/pubs/commentary/2025/07/undersea-cables-are-vulnerable-to-sabotage-but.html?utm_**

All about Security. (2025). *Group-IB veröffentlicht neuen Hightech-Crime-Report- Europa im Visier, raffinierte cyberangriffe (APTs) steigen um 58%. Retrieved Jul 20, 2025, from* **https://www.all-about-security.de/group-ib-veroeffentlicht-neuen-hightech-crime-report-europa-im-visier-raffinierte-cyberangriffe-apts-steigen-um-58/**

Antonio Albaladejo Román, Suzana Anghel, Luisa Antunes, Naja Bentzen, Julie Claustre, Mario Damen, StefanoDe Luca, Costica Dumbrava, Gregor Erbach, Clément Evroux, Myriam Goinard, Gisela Grieger, Issam Hallak, Martin Höflmayr, Liselotte Jensen, Ulrich Jochheim, Marc Jütten, Jurgita Lekaviciute, Tambiama Madiega, VirginiaMahieu, Zsolt Pataki, Guillaume Ragonnaud, Magdalena Sapala, Marcin Szczepanski, Agnieszka Widuto, AlexWilson and Ionel Zamfir. (2023). *Future Shocks 2023 Anticipating and weathering the next stroms. EPRS.*

Bach, Andreas (2025). *Interview by F. Hössle.*

Bassetto, Pierluigi (2025). *Interview by F. Hössle.*

Benner, Thorsten. (2024). *Unterseekabel: Kritsich ungeschützt. International Politik. Retrieved Aug 05, 2025, from* **https://internationalepolitik.de/de/unterseekabel-kritisch-ungeschuetzt**

Bijlagen bij COM. (2024). *Staat van het digitale decennium 2024. EU Monitor.* **https://www.eumonitor.nl/9353000/1/j4nvirkkkr58fyw_j9vvik7m1c3gyxp/vmem534xtfzl**

Blenker, Christian. (2024). *Warum Russlands Schattenflotte verdächtigt wird. Tagesschau. Retrieved Jun 15, 2025, from* **https://www.tagesschau.de/wissen/faq-unterwasserkabel-100.html**

Breukel, Paula. (2025). *Der Wasserverbrauch im Rechenzentrum hängt vom Standort ab. Datacenter Insider. Retrieved Jun 15, 2025, from* **https://www.datacenter-insider.de/der-wasserverbrauch-im-rechenzentrum-haengt-vom-standort-ab-a-%2013338c6d02e98f7ce0ec4aa04eda654b/**

Chee, Yun Foo. (2024). *EU should upgrade submarine cable infrastructure with state aid, paper says. Reuters. Retrieved Aug 5, 2025, from* **https://www.reuters.com/technology/eu-should-upgrade-submarine-cable-infrastructure-with-state-aid-paper-says-2024-02-19/?utm_**

Chestney, Nina. (2025). *EU power grid needs trillion-dollar upgrade to avert Spain-style blackouts. Reuters. Retrieved Jul 14, 2025, from* **https://www.reuters.com/sustainability/climate-energy/eu-power-grid-needs-trillion-dollar-upgrade-avert-spain-style-blackouts-2025-05-05/**

Connect Europe. (2024). *Connectivity and innovation: our report finds that Europe is at crossroads. Retrieved Jun 05, 2025, from* **https://connecteurope.org/news/connectivity-and-innovation-our-report-finds-europe-crossroads**

Connect Europe. (2025). *State of Digital Communications. Retrieved Jun 14, 2025, from* **https://connecteurope.org/insights/reports/state-digital-communications-2025**

Cyber Resilience Act. (2024). *Federal Office of Information Security. Retrieved Jun 16, 2025, from* **https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html**

Delgado, Dácil. (2025). *Competitiveness and the state of digital communications in Europe in 2025. Telefónica. Retrieved Jun 05, 2025, from* **https://www.telefonica.com/en/communication-room/blog/competitiveness-state-digital-communications-europe-2025-2/**

Deutschlandfunk. (2025). *Europa im globalen Wettrennen um Souveränität. Retrieved Jun 27, from* **https://www.deutschlandfunk.de/digital-strategie-europa-unabhaengig-usa-china-chips-clouds-100.html**

Digital Operational Resilience Act (DORA). (2025). *Eiopa European Insurance and Occupational Pensions Authority. Retrieved Jul 10, 2025, from* **https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en**

Edge Editors. (2021). *NIST cyber-resiliency framework extended to include critical infrastructure controls. DARKREADING. Retrieved Jul 10, 2025*

ENISA (A). (n.d.). *Information Sharing and Analysis Centers – Transport. Retrieved Jun 25, from* **https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/transport**

ENISA (B). (2024). *Report on the State of the cybersecurity in the Union 2024.*

ENISA (C). (2024). *Skills shortage and unpatched systems soar to high-ranking 2030 cyber threats. Retrieved Jun 25, from* **https://www.enisa.europa.eu/news/skills-shortage-and-unpatched-systems-soar-to-high-ranking-2030-cyber-threats**

ENISA (D). (2024). *Foresight 2030 Threats. Retrieved Jun 27, 2025, from* **https://www.enisa.europa.eu/sites/default/files/2024-11/Foresight%20Cybersecurity%20Threats%20For%202030%20Update%202024_0.pdf**

ENISA (E). (2024). *ENISA threat landscape 2024*.

ENISA (F). (2024). *Foresight Cybersecurity Threats for 2030 – Update executive Summary. Retrieved Jun 27, 2025, from* **https://www.enisa.europa.eu/sites/default/files/2024-11/Cybersecurity%20Threats%20for%202030%20-%20Update%202024%20-%20Executive%20Summary_0.pdf**

ENISA (G). (n.d.). *What we do. Retrieved Jun 27, 2025, from* **https://www.enisa.europa.eu/about-enisa/what-we-do?utm_ #contentList**

Euronews (2025, June 11). *Chinese-made buses in Norway can be halted remotely, spurring increased security. Euronews.* **https://www.euronews.com/next/2025/11/06/chinese-made-buses-can-be-halted-remotely-in-norway-spurring-increased-security**

European Central Bank. Retrieved Jul 05, 2025, *from* https://www.ecb.europa.eu/press/economic-bulletin/articles/2025/html/ecb.ebart202501_01~fd1781599d.en.html

European Commission, 2014. *New Study on Unlocking the ICT Growth Potential in Europe: Enabling people and businesses. Retrieved Jun 27, from* **https://digital-strategy.ec.europa.eu/en/library/new-study-unlocking-ict-growth-potential-europe-enabling-people-and-businesses?utm_**

European Commission (2020). *Investment in ICT Chapter 5.4 . Retrieved Jul 12, from* **https://ec.europa.eu/assets/rtd/srip/static/files/SRIP_2020_Chap_1.5.4.pdf?utm_**

European Commission (2024a). *Cloud Computing. Retrieved Jul 05, 2025, from* **https://digital-strategy.ec.europa.eu/de/policies/cloud-computing**

European Commission (2024b). NIS2 Directive (2024). *Retrieved Jul 10, 2025, from* **https://digital-strategy.ec.europa.eu/en/policies/nis2-directive**

European Commission (2024c). *Energy Consumption in Data Centers and Broadband Communication Networks in the EU.*

European Commission, (2024d). *The role of ICT in Critical Infrastructure Protection. Retrieved Jun 25, 2025, from* **https://cordis.europa.eu/programme/id/H2020_DS-03-2015**

European Commission (2025a). *5G Observatory Report. Retrieved Jun 20, 2025, from* **https://digital-strategy.ec.europa.eu/en/policies/5g-observatory-2025**

European Commission (2025b). *Rolling Plan for ICT standardisation. Retrieved Jun 20, 2025, from* **https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/cloud-and-edge-computing-rp-2025**

European Commission (2025c). *State of the Digital Decade 2025: keep building the EU's sovereignty and digital future. Retrieved Jun 15, 2025, from* **https://www.eu.dk/samling/20251/kommissionsforslag/kom%282025%290290/forslag/2150087/3044016/index.htm?utm_**

European Commission (2025d). *State of digital decade 2025, factsheet.*

European Commission (2025e). *2025 state of the digital decade package. Retrieved Jun 15, 2025, from* **https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package**

European Commission (n.d.). *The role of ICT in Critical Infrastructure Protection. CORDIS. Retrieved Jul 10, 2025, from* **https://cordis.europa.eu/programme/id/H2020_DS-03-2015/it**

European Federation of Engineering Consultancy Associations (EFCA) Paper on Public Procurement (2025). *Facilitating Innovation: Role of EU Public Procurement Legislation. Retrieved from:* **https://www.efcanet.org/sites/default/files/2025-06/2025-06-25_EFCA%20paper%20on%20Public%20Procurement%20%28final%29_0.pdf**

European Parliament. (n.d.). *Trans-European Networks – guidelines | Fact Sheets on the European Union | European Parliament. Retrieved November 21, 2025, from* **https://www.europarl.europa.eu/factsheets/en/sheet/135/trans-european-networks-guidelines**

Europe IT Services Market Size and Trends. (2024). *Grand view research. Retrieved Jun 15, 2025, from* **https://www.grandviewresearch.com/industry-analysis/europe-it-services-market-report**

Fabry, Elvire. (2025). *Over-dependencies in services: A blind spot in the EU economic security strategy?. Institut Jacques Delors Notre Europe. Retrieved Jul 05, 2025, from* **https://institutdelors.eu/en/publications/over-dependencies-in-services-a-blind-spot-in-the-eu-economic-security-strategy/**

Farfan, Javier; Lohrmann, Alena. *Gone with the clouds: Estimating the electricity and water footprint of digital data services in Europe. Energy Conversion and Management.*

Feasey, Richard; De Streel, Alexandre; Alexiadis, Peter; Bourreau, Marc; Cave, Martin; Godlovitch, Ilsa; Manganelli, Antonio; Monti, Giorgio; Shortfall, Tony; Timmers, Paul. (2024). *The Future of European Telecommunications: In-Deth analysis. Centre on Regulation in Europe. Retrieved Jun 24, 2025, from* **https://cerre.eu/wp-content/uploads/2024/09/CERRE_The-Future-of-European-Telecommunications-In-depth-Analysis_FINAL.pdf?utm_**

Fibre and 5G continue to expand their footprint, while fixed wireless access gains ground in OECD countries. (2025). *OECD. Retrieved Jun 27, 2025, from* **https://www.oecd.org/en/data/insights/statistical-releases/2025/05/fibre-and-5g-continue-to-expand-their-footprint-while-fixed-wireless-access-gains-ground-in-oecd-countries.html**

Filip, Marinela-Daniela, Daphne Momferatou, Rodriguez, Susana Parraga. (2025) *European Competitivness: the role of institutions and the case for structural reforms. European Central Bank. Retrieved Aug 24, 2025,* from **https://www.ecb.europa.eu/press/economic-bulletin/articles/2025/html/ecb.ebart202501_01~fd1781599d.en.html**

Forrest, Crellin. (2025). *Poor grid planning could shift Europe's data center geography, report say. Reuters. Retrieved Jul 05, 2025, from* **https://www.reuters.com/technology/poor-grid-planning-could-shift-europes-data-centre-geography-report-says-2025-06-18/**

Gatopoulos, Derek. (2024). *Europe's cybersecurity chief says disruptive attacks have doubled in 2024, sees Russia behind. AP. Retrieved Jul 20, 2025, from* **https://apnews.com/article/europe-election-cybersecurity-russia-ukraine-5b0cca725d17a028dd458df77a60440c**

Gobierno de Espana. (n.d.). Cybersecurity Operations Center (COCS). Espana digital 2026. *Retrieved Aug 15, 2025, from* **https://espanadigital.gob.es/en/measure/cybersecurity-operations-centre-cocs**

Guinea, Oscar, Vanika Sharam. (2025). *The Future of European Digital Competitiveness. ECIPE. Retrieved Jul 04, 2025, from* **https://ecipe.org/wp-content/uploads/2025/01/ECI_25_PolicyBrief_02-2025_LY03.pdf**

Güell Paule, Laia. (2023). *State of the Digital Decade Package. Digital Skills & Jobs Platform. Retrieved Jul 15, 2025, from* **https://digital-skills-jobs.europa.eu/en/actions/european-initiatives/state-digital-decade-package**

HaDEA. (2025). *Connecting Europe Facility.* https://hadea.ec.europa.eu/programmes/connecting-europe-facility_en

Hahn, Marten. (2025). *Wenn Anker und Algorithmen zur Waffe werden. DASPARLAMENT. Retrieved Aug 5, 2025, from* **https://www.das-parlament.de/aussen/europa/wenn-anker-und-algorithmen-zur-waffe-werden#:~:text=Rettungsstellen%20stellten%20ihre%20Arbeit%20ein,Prozent%20im%20Vergleich%20zum%20Vorjahr.&text=Frachter%20im%20Blick:%20Nach%20mutmaßlicher,frustrierend%20für%20die%20betroffenen%20Menschen.%22**

ICT. 2025. *ITA Italian Trade Agency. Retrieved Jul 25, 2025, from* **https://www.ice.it/en/invest/sectors/ict**

IEA. (2023). *Electricity Grids and Secure Energy Transitions, Enhancing the foundations of resilient, sustainable and affordable power systems. International Energy Agency. Retrieved Jul 16, 2025, from* **https://iea.blob.core.windows.net/assets/ea2ff609-8180-4312-8de9-494bcf21696d/ElectricityGridsandSecureEnergyTransitions.pdf**

IEA. (2025). *Energy demand for AI. Retrieved Jul 16, 2025, from* **https://www.iea.org/reports/energy-and-ai/energy-demand-from-ai?utm_**

Insikt Group. (2025). *Submarine Cables Face Increasing Threats Amid Geopolitical Tensions and limited Repair Capacity. Retrieved Aug 05, 2025, from* **https://www.recordedfuture.com/research/submarine-cables-face-increasing-threats**

Ivo Häring, Mirjam Fehling-Kasche, Natalie Miller, Katja Faist, Sebastian Ganter, Kushal Srivastava, Aishvarya Kumar Jain, Georg Fischer, Kai Fischer, Jörg Finger, Alexander Stolz Tobias Leismann, Stefan Hiermaier, Marco Carli, Federica Battisti, Rodoula Makri, Giuseppe Celozzi, Maria Belesioti, Evangelos Sfakianakis, Evita Agrafioti, Anastasia Chalkidou, George Papadakis, Clemente Fuggini, Fabio Bolletta, Alberto Neri, Guiseppe Giunta, Hermann Scheithauer, Fabian Höflinger, Dominik J. Schott, Christian Schindelhauer, Sven Köhler, Igor Linkov. (2021). *A performance-based tabular approach for joint systematic improvement of risk control and resilience applied to telecommunication grid, gas network, and ultrasound localization system. Springer.*

Jancová, Lenka; Saulnier, Jérome; Heflich, Aleksandra. (2025) *Benefits of EU strategic investment in high-tech digital innovation. EPRS European Parliamentary research service. Retrieved Aug 23, 2025, from* **https://www.europarl.europa.eu/RegData/etudes/STUD/2025/762853/EPRS_STU(2025)762853(ANN01)_EN.pdf**

Jérôme Saulnier, Aleksandra Heflich and Lenka Jančová with Iulia-Maria Florea and Karla Grosse Kohorst. (2025). *Benefits of EU strategic investment in high-tech digital innovation. European Parliament. Retrieved Jul 17, 2025, from* **https://epthinktank.eu/2025/02/12/benefits-of-eu-strategic-investment-in-high-tech-digital-innovation/**

Kehoe, L. (2025). *5G Coverage in Europe: Progress Toward Goals Amid Lingering Disparities. OOKLA. Retrieved Jun 12, 2025, from* **https://www.ookla.com/articles/europe-5g-q2-2025Cover**

Lehto, Essi; Sytas, Andrius. (2024). *Finland boards oil tankers suspected of causing internet, power cable outages. Retrieved Aug 05, 2025, from Reuters.* **https://www.reuters.com/world/europe/finland-police-investigate-role-foreign-ship-after-power-cable-outage-2024-12-26/?utm_**

Leitzcloud. (2022). *The Infrastructure of The Internet: The Submarine Cables. Retrieved Aug 05, 2025, from* **https://leitz-cloud.com/internet-cable**

Matić, Nikola (2025). *Interview by F. Hössle.*

Markopoulou, Dimitra, Vagelis Papakonstantinou. (2022). *Digitalisation of Water Services and the Water Sector- Cyber Threat Landscape: Is the EU Regulatory Framework Adequate? Journal of Water Law 27 (4).*

May, Capucine; Schwartz, Laura. (2025). *Majority of world's top data centre hubs face array of rising heat-related risks. Verisk. Retrieved Jul 23, 2025, from* **https://www.maplecroft.com/products-and-solutions/sustainable-supply-chain/insights/majority-of-worlds-top-data-centre-hubs-face-array-of-rising-heat-related-risks/**

Ministerio Para la Transformación digital y de la función pública. (2025). *The Government approves a strengthening of Spain's cybersecurity and cyberdefence capabilities with 1,157 million euros. Retrieved Jul 04, 2025, from* **https://digital.gob.es/en/comunicacion/notas-prensa/mtdfp/2025/05/2025-05-06_02**

NIS Cooperation Group. (2023). *EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors.*

Pidgeon, Andrew (2025). *Interview by F. Hössle*.

RENO. (2025). *European Cloud Providers' local market share now holds steady at 15%. Synergy research group. Retrieved Jul 05, 2025, from* **https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15**

Reuters (2025, September 22). *EU agency confirms ransomware attack behind airport disruptions. Reuters Media.* **https://www.reuters.com/business/aerospace-defense/eu-agency-says-third-party-ransomware-behind-airport-disruptions-2025-09-22/**

Rolofs, Oliver. (2022). *Warum Europa seine Schwachstelle Unterseekabel dringend beheben muss. Focus online. Retrieved Aug 05, 2025, from* **https://www.focus.de/finanzen/news/das-zeitalter-der-kabel-die-groesste-achillesferse-des-westens-liegt-in-4000-metern-tiefe_id_180247998.html**

Ross, Ron; Pillitteri, Victoria; Graubart Richard; Bodeau, Deborah; Mcquaid, Rosalie. (2019). *Developing Cyber Resilient Systems: A Systems Security Engineering Approach. U.S. Department of Commerce.*

Schweinar, Andreas (2025). *Interview by F. Hössle.*

Silicon Editorial. (2023) Gartner: IT Spending in Europe to Rise by 9% in 2024. *Silicon Technology Powering Business. Retrieved Jul 05, 2025, from* **https://www.silicon.eu/gartner-it-spending-in-europe-to-rise-by-9-in-2024-11480.html**

Silicon Saxony. (2025). *Bevor Europa aus allen Wolken fällt – Problemzone „Europäische Cloud-Infrastrukturen". The High-Tech Network. Retrieved Jul 06, 2025, from* **https://silicon-saxony.de/bevor-europa-aus-allen-wolken-faellt-problemzone-europaeische-cloud-infrastrukturen/**

Telecom Review. (2024). *Heatwaves: A major Telecommunications Industry Threat. The Telecom Industry's Media Platfrom. Retrieved Aug 03, 2025, from* **https://telecomreview.com/articles/reports-and-coverage/8236-heatwaves-a-major-telecommunications-industry-threat/**

Soller, Henning (2025): *The Year of Quantum: From concept to reality in 2025. In McKinsey & Company, 23/6/2025. Retrieved 01/10/2025 from:* **https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025#/**

Vertiv, Jon Abbott. (2025). *AI workloads are reshaping infrastructure – here's what data centers need to know. Techradar pro. Retrieved Aug 03, 2025, from* **https://www.techradar.com/pro/ai-workloads-are-reshaping-infrastructure-heres-what-data-centers-need-to-know**

Villalobos, José María Riverira; Serrano, Álvaro Gutiérrez. (2024). *5G national security framework: boosting network security. Telefónica. Retrieved Jul 13, 2025, from* **https://www.telefonica.com/en/communication-room/blog/5g-national-security-framework-boosting-network-security/**

Voce, Antonio; Ahmedzade, Tural; Kirk, Ashley. (2025). *Shadow fleets and subaquatic sabotage: re Europe's undersea internet cables under attack? The Guardian. Retrieved Aug 05, 2025, from* **https://www.theguardian.com/world/ng-interactive/2025/mar/05/shadow-fleets-subaquatic-sabotage-europe-undersea-internet-cables-under-attack?utm_**

Voice&Data. (2024). *Early warnings in the heatwave mine: Telecom at risk. Retrieved Aug 03, 2025, from* **https://www.voicendata.com/telecom-infra/early-warnings-in-the-heatwave-mine-telecom-at-risk-6950641**

Wakoba, Sam. (2022). *Kenya government to install 100 kms of fibre optic cables & 25.000 Internet Hotspots to spur economic growth. TECHMORAN. Retrieved Aug 15, 2025, from* **https://techmoran.com/2022/04/14/kenya-government-to-install-100kms-of-fiber-optic-cables-25000-internet-hotspots-to-spur-economic-growth/**

Weyerts, Isabel. (2025). *Handelsabkommen zwischen EU und USA verfestigt die technologische Abhängigkeit Europas. Bundesverband IT-Mittelstand e.V. Retrieved Jul 10, 2025, from* **https://bitmi.de/handelsabkommen-zwischen-eu-und-usa-verfestigt-die-technologische-abhaengigkeit-europas/**

Wodecki, Ben. (2025). *Data: 81% of telecos admit aging infrastructure slowing innovation. Capacity a techoraco brand. Retrieved Jun 23, 2025, from* **https://www.capacitymedia.com/article/data-81-of-telcos-admit-aging-infrastructure-slowing-innovation**

efca
European Engineering Consultancies

Engineering Resilience

**EFCA Secretariat**
Avenue des Arts 3/4/5, B-1210 Brussels
Phone: + 32 (0)2 209 07 70
email: efca@efca.be
http://www.efcanet.org