Hard facts. Clear stories.

Copenhagen Economics

THE TELECOM SECTOR'S CONTRIBUTION TO EUROPE'S SECURITY AND RESILIENCE

COMMISSIONED BY CONNECT EUROPE
OCTOBER 2025

ABOUT COPENHAGEN ECONOMICS
Copenhagen Economics is an expert-driven consulting company built on a deep knowledge of applied economics, and one of the leading economics firms in Europe.

We believe sound economic analysis can equip decision makers with hard facts and clear stories to make better choices for the benefit of society. We are committed to delivering compelling and pragmatic economics solutions with a creative and candid approach.

A brief note on consultancy research
As is standard in our field of professional services, research is designed so that:

- the client chooses the research question;
- we analyse and address the question to the best of our knowledge;
- findings and conclusions are our own.

The independence of our professional services is ensured via a diversified portfolio of business, spanning public sector and private clients across industries. For further information, see www.copenhageneconomics.com. We remain available for and appreciate any questions or comments.

PREFACE

Telecom networks provide key infrastructure, enabling everything from daily communications to business operations and government services. With digital dependency deepening across Europe, and in the context of an evolving risk landscape, the security and resilience of telecom networks has never been more important. Despite the importance of this topic, there are few studies that cover security and resilience in the context of telecom networks.

Against this backdrop, Connect Europe commissioned Copenhagen Economics to develop a study explaining the importance of security and resilience to end-users and society at large and the specific measures that telecom operators implement to ensure security and resilience. Furthermore, the study explores which actions policymakers should consider to ensure continued security and resilience.

The study is based on comprehensive desk research as well as interviews with security professionals at seven European telecom operators (Deutsche Telekom, KPN, Orange, Telecom Italia, Telefónica, Telenor, and United Group) and two vendors (Ericsson and Nokia). For simplicity, the study treats European telecom operators as a broad category, despite differences in size, market position, and business models. While it does not segment operators by type, the goal is to cover security and resilience efforts that are common across the sector.

This study also focuses specifically on network operators' security and resilience measures and does not consider measures taken elsewhere in the communication service value chain. However, it is important to acknowledge that security and resilience challenges extend well beyond telecom networks alone, encompassing interconnected systems across all layers of the value chain such as downstream cloud infrastructure and end-user devices.

Table of contents

THE TELECOM SECTOR'S CONTRIBUTION TO SECURITY AND RESILIENCE IN EUROPE

Copenhagen Economics

STUDY BY COPENHAGEN ECONOMICS FOR CONNECT EUROPE

Telecom networks provide critical infrastructure. This study explores security and resilience in European telecom networks - a topic of increasing importance to society and end-users - based on desk research and interviews with operators and vendors.

SECURE AND RESILIENT TELECOM NETWORKS BENEFIT END-USERS AND SOCIETY

- SEAMLESS ACCESS TO DOWNSTREAM SERVICES
- PROTECTION OF PERSONAL AND SENSITIVE INFORMATION
- ENABLING CRITICAL SECTORS
- SUPPORT ECONOMIC GROWTH AND WIDER SOCIETAL BENEFITS

DELIVERING SECURE AND RESILIENT NETWORKS REQUIRES NAVIGATING A COMPLEX RISK LANDSCAPE

- SYSTEM FAILURES
- THIRD-PARTY FAILURES
- HUMAN ERRORS
- MALICIOUS ACTIONS
- NATURAL PHENOMENA

HOW DO TELECOM OPERATORS ENSURE SECURE AND RESILIENT NETWORKS?

"**SECURITY IS IN OUR DNA**. IT CANNOT BE IMPLEMENTED AS AN AFTERTHOUGHT - BUT MUST BE INTEGRATED IN ALL SYSTEMS AND PROCESSES FROM THE START."

- Security expert at a major European telecom operator.

TELECOM OPERATORS ENGAGE IN A COMPREHENSIVE SET OF SECURITY AND RESILIENCE MEASURES

SECURITY

Measures to avoid and prevent attacks, breaches, or other forms of interruptions

- Personnel training
- Physical protection
- Threat detection
- Vulnerability assessment
- Access management
- Secure hardware and software

RESILIENCE

Measures that avoid or minimise any impact for end-user when an incident occurs

- Business continuity
- Disaster recovery
- Incident management
- Continuous learning

POLICY OPPORTUNITIES TO SUPPORT CONTINUED SECURITY AND RESILIENCE

- **SUPPORT INVESTMENT IN SECURITY AND RESILIENCE**
- **STREAMLINE REGULATION**
- **ADDRESS SKILL SHORTAGES**

EXECUTIVE SUMMARY

Telecom networks serve as the backbone of modern society, supporting essential functions ranging from daily communications to essential public and private services. Citizens, businesses, and governments are increasingly dependent on these networks, which are interconnected with critical sectors such as energy, healthcare and finance. Security and resilience are essential conditions for telecom networks to deliver substantial end-user benefits, productivity gains and economic growth. However, operators navigate an increasingly complex risk landscape with five main types of risks: system failures, third-party failures, natural phenomena, human errors, and malicious actions (cyber threats and physical sabotage). To manage these risks, telecom operators have integrated a comprehensive set of security and resilience measures into their everyday operations.

Security measures seek to protect against attacks, breaches, or other forms of interruptions, and include: automated threat detection, continuous vulnerability scanning, physical protection of sites and assets, and ongoing personnel training and innovation efforts. Operators also enable security for end-users through services like DDoS protection, anti-spoofing, and anti-fraud solutions. In addition, some operators offer managed security services directly to their customers on a commercial basis.

Resilience measures seek to minimise the impact on end-users in the event of breaches, disruptions, or downtime. These include business continuity measures (such as network redundancies, backup power, and data backups for some part of the network), around-the-clock incident management processes, regularly tested disaster recovery plans coordinated with public entities, and intelligence sharing across the sector to ensure systematic learning from incidents.

Telecom operators exert significant resources to ensure security and resilience, with these costs embedded throughout all network operations and difficult to quantify precisely. These costs are expected to rise substantially due to evolving threats and policy requirements.

Despite these significant efforts by operators, our study identifies **several structural and operational challenges, underscoring the need for targeted policy actions**.

Potential policy actions to strengthen security and resilience further:

- ***Support investment in security and resilience*** to address financial pressures through appropriate policy frameworks, considerations of their role in merger assessments where appropriate, and public support where public interests extend beyond commercial considerations
- ***Streamline regulation*** to reduce administrative burden from overlapping requirements between sector-specific regulations and horizontal frameworks and address duplicate reporting requirements
- ***Address skill shortages*** to alleviate Europe's shortage of skilled cybersecurity professionals by developing a future-proof EU cybersecurity skill strategy

CHAPTER 1

SECURE AND RESILIENT TELECOM NETWORKS SUPPORT SUBSTANTIAL BENEFITS FOR END-USERS

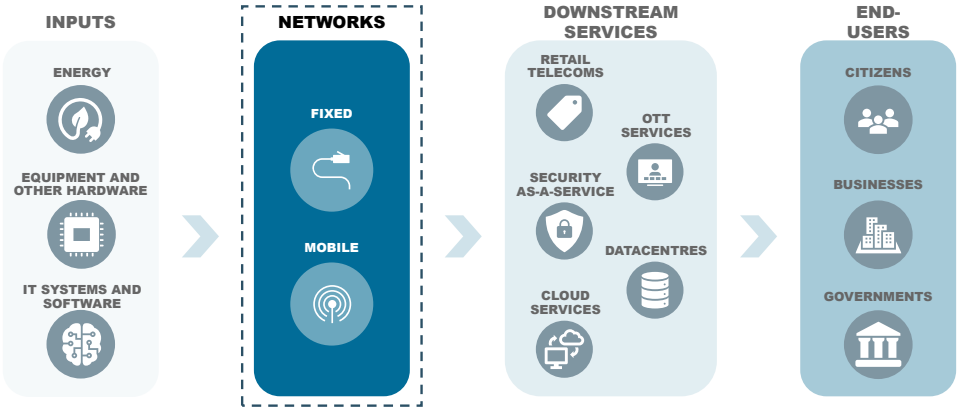
An increasing part of economic and civil activity, as well as public services, relies on digital communications, such as payments, online banking, everyday communications, and other digital services. Fixed and mobile telecom networks (hereafter 'telecom networks') provide key infrastructure that enable these downstream activities and support substantial benefits for end-users. The security and resilience of this infrastructure is essential to protect data and ensure the continuation of operations across society.

In this chapter, we first describe how telecom networks form the basis of the communication services value chain and the benefits they support for end-users, as secure and resilient networks contribute to productivity gains and economic growth by ensuring reliable services for citizens, businesses, and governments (Section 1.1). We then examine the types of risks telecom operators must navigate (Section 1.2).

1.1 SECURE AND RESILIENT TELECOM NETWORKS PLAY A KEY ROLE IN SUPPORTING THE ECONOMY

Telecom networks are crucial to enable a wide range of communication and digital services that benefit businesses, governments, and citizens, see Figure **1**. The communication services value chain spans from upstream inputs to telecom networks, and further to downstream services and ultimately to end-users. This study focuses on fixed and mobile operators. We do not focus on satellite and subsea cable providers.

Figure 1
Telecom networks are the foundation of the communication services value chain



Note: In this study, we focus on the layer with networks and only briefly touch upon the other layers. OTT ('over-the-top') services are digital distribution services of video and audio delivered directly to viewers via the internet, rather than through traditional channels.
Source: Copenhagen Economics.

During recent decades, connectivity has expanded in both coverage and capability, such that fixed and mobile networks now support widespread high-capacity connectivity. High-speed technologies, such as 5G networks and Very High Capacity Networks (VHCN),[1] have been rolled out rapidly in recent years and thereby enabled digital transformation across sectors and countries. 5G mobile coverage has grown from 14 per cent of EU households in 2020 to 89 per cent in 2023 and VHCN fixed coverage has grown from 60 per cent to 79 in the same period.[2]

Telecom networks support important services to end-user

Telecom networks support a wide range of important downstream services such as retail telecoms, OTT services, security as-a-service, data centres, and cloud services. Without telecom networks, these downstream services would not be possible. These services benefit end-users across the economy, including: **citizens, businesses,** and **governments.**[3]

Citizens benefit extensively from connectivity in daily life. In 2024, 88 per of EU citizens used the internet daily, which is an increase of 52 percentage points since 2007.[4] Citizens use the internet for a range of activities, with 77 per cent making online purchases and 72 per cent used online banking in 2024. Additionally, the use of connected devices is widespread: two in three internet users report using Internet of Things (IoT) devices such as smart home systems, wearables, or connected vehicles.[5] These figures demonstrate that everyone benefits extensively from secure and resilient telecom networks and the services they enable. The importance of telecom networks will only become greater with increased digitalisation.

1 BEREC (2025, website), What are Very High Capacity Networks? (link). In practice, this is mostly fibre-to-the-premises (FTTP).
2 Eurostat (2025, website), Broadband internet coverage by technology (online data code: isoc_cbt, link).
3 See e.g., Okoro et al. (2024), Digital communication and U.S. economic growth: a comprehensive exploration of technology's impact on economic advancement (link).
4 Eurostat (2025, website), Individuals - frequency of internet use (online data code: isoc_ci_ifp_fu, link).
5 Eurostat (2025), Digitalisation in Europe – 2025 edition (link).

Businesses across all sectors also benefit extensively from connectivity and depend on telecom networks for day-to-day operations. In 2024, 99 per cent of European businesses had access to the internet and 53 per cent engaged in online meetings. Additionally, many businesses are becoming increasingly reliant on e-commerce, with 24 per cent of revenue in 2024 coming from e-commerce, see Figure **2**.

Figure 2
European businesses rely extensively on the internet
Per cent of European businesses with at least 10 employees in 2024

Note: The figure shows the percentage of Europeans businesses with at least 10 employees who have access to the internet, who engage in online meetings, and the share of their revenue that stem from e-commerce.
Source: Eurostat (2025, website), Internet access by size class of enterprise (online data code: isoc_ci_in_es, link); Eurostat (2025, website), Meetings via the internet by size class of enterprise (online data code: isoc_ci_mvis, link); and Eurostat (2025, website), Value of e-commerce sales by NACE Rev. 2 activity(online data code: isoc_ec_evaln2, link).

Secure and resilient telecom networks are especially important for critical sectors. As noted by the NIS Cooperation Group: *"In terms of spillover from the telecommunications sector to other sectors, all critical sectors are highly dependent on the availability of telecommunications."*.[6] This dependency means that providers of essential services fundamentally rely on secure and stable telecom networks to operate effectively. For example:

- The energy sector increasingly depends on telecom infrastructure for key operational and strategic functions. The EU project ENERGISE mapped these dependencies using data from nearly all EU member states, highlighting how telecom networks support a range of critical applications. These include smart metering with real-time data and remote billing, grid operation through monitoring and predictive maintenance, and integration of decentralised renewables that rely on constant data exchange and control.[7]
- The financial services sector increasingly relies on digital infrastructure. Disruption in the telecom sector could disrupt digital payments, which would in turn affect people's ability to buy essentials, such as food.[8] Such dependencies became clear in May 2025 in Spain, when a mobile network outage due to a power cut caused issues for online and mobile payments, frustrating both consumers and businesses.[9]

6 NIS Cooperation Group (2023), EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors, page 19 (link).
7 ITU (2017), ICT for ENERGY – Telecom and Energy Working Together for Sustainable Development (link).
8 NIS Coorperation Group (2024), Cybersecurity and resiliency of Europe's communications infrastructures and networks (link).
9 See e.g., Finextra (2025), Spanish mobile networks go dark (link).

- The health sector would be affected by an outage in telecom services since the sector rely on online services to retrieve online health information of patients, access the internet to diagnose patients, and to schedule appointments.[10]
- The transportation sector relies on communications to monitor and control the flow of ground, sea, and air traffic.[11]

Governments also benefit extensively from telecom networks to operate and to deliver digital services to citizens. In 2023, 69 per cent of EU citizens used a website or an app of public authorities and 41 per cent used electronic identification, see Figure **3**.

Figure 3
European governments rely on digital services to interact with citizens
Per cent of European citizens in 2023

Note: The figure shows the percentage of Europeans citizens who used a website or an app of public authorities and who used electronic identification for private purposes in 2023.
Source: Eurostat (2025, website), E-government activities of individuals via websites (online data code: isoc_ciegi_ac, link) and Eurostat (2025, website), Use of electronic identification (eID) (online data code: isoc_eid_ieid, link).

Secure and resilient telecom infrastructure also supports national security and emergency response systems. For example:

- Governments rely on telecom networks for secure communications between countries including exchange of sensitive information. [12]
- Emergency services such as emergency calls and public warning systems rely on telecom services and could be disrupted if the telecom network experienced disruptions. This dependency became clear in Denmark in November 2024, when a breakdown in telecom services left almost three million Danes unable to make calls – including emergency calls – for multiple hours.[13]

[10] NIS Coorperation Group (2024), Cybersecurity and resiliency of Europe's communications infrastructures and networks (link).
[11] Cybersecurity & Infrastructure Security Agency (2025, website), Communications Sector (link).
[12] NIS Coorperation Group (2024), Cybersecurity and resiliency of Europe's communications infrastructures and networks (link).
[13] DR (2024), Massivt nedbrud hos TDC skabte 112-kaos: Nu lover Teleindustrien forbedringer (link).

Security and resilience are essential conditions for the telecom network's ability to deliver substantial end-user benefits

Secure and resilient telecom networks support continued benefits to citizens, businesses, and governments by ensuring seamless access to downstream services, protecting personal and sensitive information, and enabling critical sectors. Additionally, they support economic growth and wider societal benefits, see Figure **4**.

Figure 4
Telecom networks provide several benefits to end-users: citizens, businesses and governments

Source: Copenhagen Economics.

For **citizens**, secure and resilient networks unlock seamless access to everyday digital services such as messaging, streaming, banking, and online purchases, while ensuring emergency services remain reliably accessible.[14] Strong data protection enables users to confidently use digital tools, knowing their personal information remains private and secure from manipulation.

For **businesses** – including critical sectors – and **governments**, secure and resilient networks provide the reliable foundation needed to maintain operations and deliver essential services efficiently. For companies within critical sectors such as finance, energy, and transport this reliability enables them to serve society effectively[15] and robust data protection safeguards commercial innovations and sensitive citizen information. Strong cybersecurity infrastructure prevents systemic risks and supports business continuity,[16] as demonstrated by lessons learned from incidents like the CrowdStrike breakdown in 2024, where a faulty update in their cloud-based security software affected governments and businesses around the world.[17] Although difficult to quantify, one estimate by the technology consultancy Parametrix suggests that Fortune 500 companies faced more than USD 5 billion in financial losses due to the CrowdStrike outage.[18] This incident and the substantial associated losses illustrate the value of connectivity in the modern economy, as different companies and sectors face significant financial consequences when wider outages happen.

14 NIS Coorperation Group (2024), Cybersecurity and resiliency of Europe's communications infrastructures and networks (link).
15 NIS Coorperation Group (2024), Cybersecurity and resiliency of Europe's communications infrastructures and networks (link).
16 Based on interviews with security professionals in European telecom operators.
17 World Economic Forum (2025), Global Cybersecurity Outlook 2025 (link).
18 Parametrix (2024), CrowdStrike's Impact on the Fortune 500 – An Impact Analysis (link).

Overall, the communication service value chain – including secure and resilient telecom networks – contributes to **economic growth** by supporting productivity, business efficiency, innovation, and enabling new services and business models.[19] Several studies link increases in broadband adoption and speed to higher GDP growth. For example, one study finds that a 100 per cent increase in broadband download speed results in a GDP increase of 0.26-0.73 per cent,[20] and another finds effects as high as a 1.97 per cent increase in GDP.[21]

Telecom networks not only support productivity and economic growth via positive spillovers to adjacent sectors,[22] they also support **wider societal benefits**. These include seemingly unrelated areas, such as emission reductions. Estimates from The World Economic Forum suggest that ICT solutions, and in particular 5G, could "*help reduce global carbon emissions by up to 15% – or one-third of the 50% reduction required by 2030 – through solutions in energy, manufacturing, agriculture and land use, buildings, services, transportation and traffic management*."[23]

1.2 TELECOM OPERATORS MUST NAVIGATE A COMPLEX RISK LANDSCAPE

Telecom operators face an increasingly complex and widespread landscape of risks.[24] As the role of communication services has grown, so has the scope of risks that operators must manage. Additionally, the geopolitical landscape has shifted in recent years, reshaping the risk environment for telecom operators and increasing the need for cross-border cooperation.

> The cybersecurity threat landscape has become and continues to be significantly more complex and widespread.

Source: ENISA (2024), 2024 Report on the State of the Cybersecurity in the Union (link), page 14.

The European Commission has defined an incident taxonomy which distinguishes between five causes of incidents or types of risks. These are: system failures, natural phenomena, human errors, malicious actions, and third-party failures, see Table **1**.

19 See e.g., Briglauer, Krämer, and Palan (2023), Socioeconomic benefits of high-speed broadband availability and service adoption: A survey (link). They find that increased broadband adoption leads to positive effects in product innovation, technological progress, and efficiency gains. These positive effects ultimately lead to an impact on GDP.

20 Telecom Advisory Services (2020), Assessing the Economic Potential of 10G Networks (link). They find that a 100 per cent increase in fixed broadband download speed results in a GDP increase of 0.26 per cent for download speeds below 40 Mbps, and a 0.73 per cent increase for download speeds above 40 Mbps.

21 Kongaut and Bohlin (2017), Impact of broadband speed on economic outputs: An empirical study of OECD countries (link).

22 See e.g., Giroud et al. (2021), Propagation and Amplification of Local Productivity Spillovers (link), who show that local productivity boosts increase productivity further in local firms and in firms located further away.

23 World Economic Forum (2019), Digital technology can cut global emissions by 15%. Here's how (link).

24 ENISA (2024), 2024 report on the state of cybersecurity in the union (link), page 14.

Table 1
Telecom operators face five causes of incidents

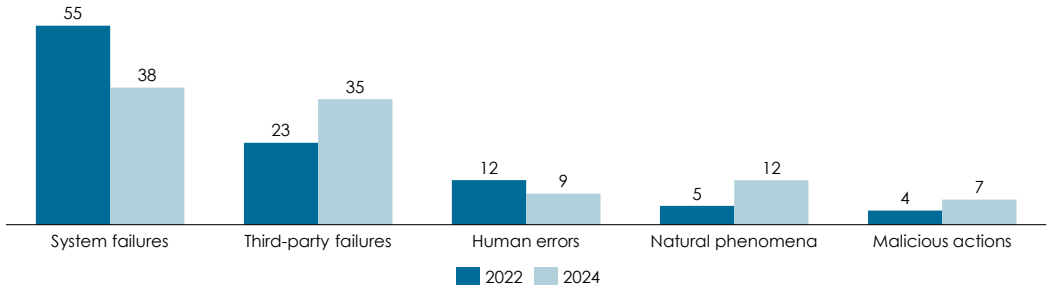
CAUSE OF INCIDENT	DESCRIPTION
System failures	• Incidents without external causes such as a hardware failure, software error, or a flaw in a procedure triggering an incident
Third-party failures	• Incidents triggered by a disruption of a third-party service such as a power outage (i.e. a supply-chain disruption)
Natural phenomena	• Incidents due to natural phenomena such as a storms, floods, or earthquakes
Human errors	• Incidents following a human error or mistake such as situations where a system worked correctly, but was used wrongly
Malicious actions	• Incidents caused by malicious actors such as a cyber-attack or physical attack

Source: European Commissions (2018), Cybersecurity Incident Taxonomy (link), page 9.

In 2024, European telecom operators reported 188 significant incidents leading to 1.7 billion lost user hours[25] relative to 155 significant incidents in 2022 leading 11.2 billion lost user hours, as reported by ENISA.[26] In 2024, system failures were the largest cause of the incidents (38 per cent), followed by third-party failures (35 per cent), natural phenomena (12 per cent), human errors (9 per cent), and malicious actions (7 per cent). From 2022 to 2024, the largest increase in significant incidents appear to be driven by events that stem from outside of the telecom networks themselves, such as third-party failures and natural phenomena,[27] see Figure **5**.

[25] ENISA (2025), Telecom security incidents 2024 (link).
[26] ENISA (2023), Telecom security incidents 2022 (link).
[27] This picture also seem to be the case from 2023 (with 156 incidents) to 2024 even though we do not have the complete dataset, see ENISA (2025), Telecom security incidents 2024 (link).

Figure 5
System failures and third-party failures are the largest sources of significant incidents
Per cent of significant incidents reported by telecom operators in 2022 and 2024



Note: ENISA breaks down the incidents caused by third-party failures into failures caused by one of the other four causes (system failures, natural phenomena, human errors, or malicious actions). We count the third-party failures as a separate category, since it is a distinct type of risk that operators face and plan for (e.g. through power back-ups). In 2024, most third-party failures were caused by system failures (77%), followed by human errors (11%), malicious actions (9%), and natural phenomena (3%). It was similar in 2024 with system failures (65%), human errors (29%), malicious actions (3%), and natural phenomena (3%). We have not included data from 2023 since the breakdown of third-party failures is not available and can thus not be filteredout from the other categories.
Source: Copenhagen Economics based on ENISA (2025), Telecom security incidents 2024 (link) and ENISA (2023), Telecom security incidents 2022 (link).

Data suggests that the resilience of telecom networks is improving. Despite ENISA reporting a record-high incidents in 2024, user hours lost fell by 55 per cent compared to 2023 (and 85 per cent compared to 2022), suggesting "*the possibility of improved outage management, enhanced infrastructure and increased system resilience*".[28] This aligns with operators' reports of preventing millions of attempted attacks daily without causing significant incidents through robust security measures.[29] Notably, the frequency of incidents does not necessarily reflect the relative severity of different risks.

Below, we describe each of the five causes of incidents (risks) and present examples and learnings of select incidents.

System failures
System failures are defined as incidents without external causes such as a hardware failure, software error, or a flaw in a procedure triggering an incident.

For example, in 2024, a breakdown in the Danish telecom network was caused by two independent technical errors – a faulty function update and a software error – which would not have been serious in isolation. In combination these led to a breakdown in services where hundreds of thousands of Danes were not able to make calls for more than six hours.[30]

[28] ENISA (2025), Telecom security incidents 2024 (link), p.3
[29] See for example Deutsche Telekom (2024), Tense cyber situation: Telekom expands protection center (link).
[30] Berlingske (2024), Nu afslører TDC årsagen til det store mobilnedbrud – og det burde ikke kunne ske (link).

Third-party failures

Third-party failures are defined as incidents triggered by a disruption of a third-party service such as a power outage (i.e. a supply-chain disruption). The telecom sector – alongside most modern sectors – is particularly dependent on stable power supply. Despite power backups, failures upstream in the energy sector can lead to cascading effects on network operations, ultimately affecting downstream services that rely on connectivity. Telecom networks are intertwined with different critical sectors and failures can spill over from one to another.

Natural phenomena

Natural phenomena are defined as incidents due to natural phenomena such as a storms, floods, or earthquakes. These events can damage physical infrastructure leading to outages.

For example, in January 2025 in Ireland, Storm Éowyn caused extensive damage to both the energy grid and telecom networks, leaving 10 per cent of fixed and 35 per cent of mobile users without service.[31] Telecom operators mitigated the impact of the storm in Ireland by preparing for the damages beforehand and by allocating all available resources to repair the damages when the storm lifted, showing that timely planning can reduce the impact on consumers.[32] Following the storm, public authorities have sought input from telecom operators to identify the key impacts of climate change on communication networks, which will help develop a response strategy for any future events.[33]

These risks are expected to grow as climate-related events become more frequent.

Human errors

Human errors are defined as incidents following a human error or mistake such as situations where a system worked correctly but was used wrongly. Mistakes in configuration, maintenance, or operational procedures can introduce vulnerabilities or cause outages. In addition, malicious actors often seek to exploit human mistakes through tactics like phishing, spear-phishing, and social engineering. Thus, operators must have systems, training and safeguards in place to minimise both the risk and impact of such mistakes.

Malicious actions

Malicious actions are defined as incidents caused by malicious actors, such as a cyber-attacks or physical attacks. These risks are evolving quickly, driven by technological developments and growing geopolitical tensions, and operators continuously adapt their defences to ensure confidentiality, integrity, and availability of data and systems.

31 The Irish Times (2025), Plan under way to protect telecoms network from extreme weather (link).
32 Openreach (2025), Storm Eowyn (link).
33 The Irish Times (2025), Plan under way to protect telecoms network from extreme weather (link).

> Malicious cyber activity has become a clear component of wider hybrid threats, such as disinformation and physical acts of sabotage and violence, seeking to undermine and destabilise EU society, democracy and values.

Source: ENISA (2024), 2024 Report on the State of the Cybersecurity in the Union (link), page 14.

Cyber threats from malicious actors can be both economically and politically motivated. Some target sensitive data, for example through ransomware or espionage. In some cases, attackers apply a 'steal now, decrypt later' strategy, where they steal encrypted data with the expectation of breaking the encryption in the future when new technology is available, such as quantum computers, capable of breaking most commonly used public-key encryption protocols.[34] Others aim to disrupt services, such as through Distributed Denial-of-Service (DDoS) attacks where systems are overwhelmed by a flood of internet traffic such that it cannot function intentionally.[35]

Data suggests that the risk of attacks that target the availability of services has increased in recent years, with DDoS attacks growing from 28 per cent of all registered incidents in Europe in 2023[36] to 46 per cent in 2024.[37]

Physical threats to telecom infrastructure have become more relevant in recent years and are increasingly used as political statements or to disrupt connectivity. These types of incidents are primarily politically driven. Some are carried out by activist groups and individuals — for example, vandalism of Dutch 5G towers in response to alleged health concerns[38], cutting of French fibre optic cables to oppose the digitalisation of society,[39] and more recently the sabotage of more than 30 Swedish cell towers.[40] Others are linked to state-sponsored operations, including sabotage of subsea cables, see Box 1.

34 Based on interviews with security professionals in European telecom operators.
35 See e.g., Cloudflare (2025, website), What is a DDoS attack? (link) for a description.
36 Data covers the period July 2022 – June 2023, see ENISA (2023), ENISA Threat Landscape 2023 (link), page 12.
37 Data covers the period July 2023 – June 2024, see ENISA (2024), ENISA Threat Landscape 2024 (link), page 12.
38 Reuters (2020), Dutch telecommunications towers damaged by 5G protestors: Telegraaf (link).
39 Cyberscoop (2022), String of attacks on French telecom infrastructure preceded April attack on fiber optic cables (link).
40 SVT (2025), Granskning: Angrepp mot 30-tal telemaster – utreds som sabotage (link).

Box 1 Sabotage of subsea cables

Subsea data cables are fibre-optic cables lying on the seabed used to transmit digital data between countries and continents. They are among the most critical components of global internet infrastructure, carrying over 97 per cent of the world's internet traffic.

Recent years have seen a growing number of incidents involving damage to subsea data and power cables across Europe. Disruptions to subsea cables can have serious consequences. They can affect power supply, slow or block cross-border internet traffic and communications and affect international financial transactions.

The protection of undersea infrastructure typically falls under the responsibility of national authorities and defence institutions, not telecom operators even though some operators have an ownership stake in certain subsea cables. Therefore, it is outside the direct scope of this study, but the trend highlights the importance of wider protection of physical infrastructure.

For example, several disruptions in the Baltic Sea are suspected to be part of hybrid warfare tactics linked to Russian state interests, and these developments have led NATO to increase surveillance and launch dedicated missions such as *Baltic Sentry* to protect critical subsea infrastructure.

Source: ENISA (2023), Subsea Cables – what is at stake? (link); AP (2025), At least 11 Baltic cables have been damaged in 15 months, prompting NATO to up its guard (link); The Guardian (2025), 'Shadow fleets' and subaquatic sabotage: are Europe's undersea internet cables under attack? (link).

CHAPTER 2

TELECOM OPERATORS ENGAGE IN A COMPREHENSIVE SET OF SECURITY AND RESILIENCE MEASURES

Telecom operators play a central role in protecting the communication services value chain. They ensure that networks remain secure and resilient when facing deliberate attacks, accidents, or external disruptions.

In this chapter, we firstly explain the two concepts of security and resilience in relation to telecom networks and provide an overview of types of measures employed (Section 2.1). Secondly, we examine in more detail which specific measures telecom operators implement to ensure security (Section 2.2) and resilience (Section 2.3). Finally, we explore how costly it is for operators to ensure that networks are secure and resilient (Section 2.4).

We focus on efforts by telecom network operators themselves and do not consider measures taken elsewhere in the communication service value chain — for example within downstream services or by end-users, see Figure **1**.

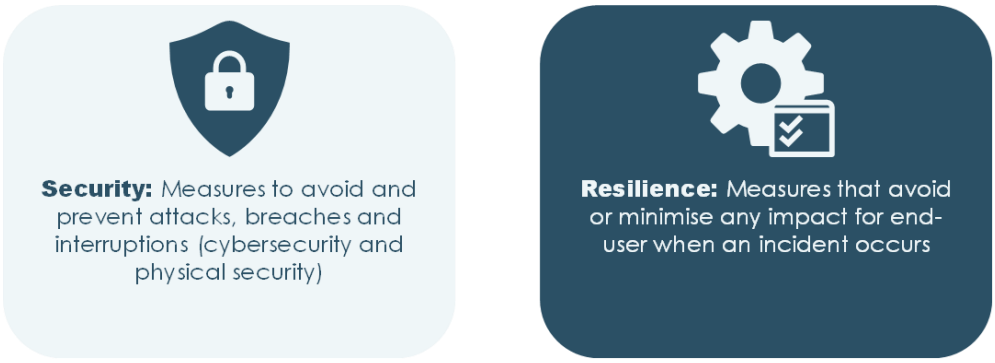
However, it is important to acknowledge that security and resilience challenges extend well beyond telecom networks alone, encompassing interconnected systems in all layers of the value chain, such as downstream cloud infrastructure and end-user devices. From the end-user perspective, security and resilience across all these interconnected elements is important and end-users may not be able to distinguish whether an issue originates at the network level, within downstream cloud infrastructure, from device vulnerabilities, or elsewhere in the value chain. While our analysis concentrates on the network layer, comprehensive security and resilience requires coordinated efforts across all interconnected components.

2.1 SECURITY MEASURES PROTECT; RESILIENCE MEASURES MINIMISE IMPACT

Security and resilience are closely linked in telecom operations, making it difficult to precisely categorise measures as relating exclusively to either security or resilience. Some operators note that the term 'resilience' is often used to refer to an end-to-end concept covering all measures that reduce the risk of breaches as well as mitigate end-user impacts in case they occur.

For the purpose of this study, we treat security and resilience as two distinct concepts to facilitate clearer description of the different type of measures employed, acknowledging that there can be substantial overlap. We use the term **security** to cover measures that avoid and prevent attacks, breaches, or other forms of interruptions. We use the term **resilience** to cover measures that avoid or minimise any impact for end-user when an incident occurs – this includes measures that ensure service continuity (e.g. via parallel infrastructure) and rapid recovery, see Figure **6**.

Figure 6
Conceptual distinction between security and resilience



Source: Copenhagen Economics based on interviews with security professionals in European telecom operators and own research.

Our use of the terms security and resilience is broadly consistent with concepts that are defined and implemented across different regulatory environments. See Box A**1** in Appendix A for an overview of definitions used by ENISA and as established in NIS2 and ISO27001.

Operators implement numerous measures to ensure security and resilience, often using risk assessments to guide their efforts, such that most resources are prioritised to the areas where risks and consequences of incidents are the greatest.

Several regulatory requirements, such as NIS2, are already in place setting obligations for operators, both in terms of risk assessments and concrete measures.[41] Additionally, voluntary standards like ISO27001 play a role in guiding efforts, and the standards often align with, or even go beyond, regulatory requirements and are widely used as a framework for structuring internal security and resilience efforts.[42]

Finally, operators respond to demand from end-users, particularly businesses and governments, who are often more explicit in their demand for security and resilience than citizens, often leading to security and resilience measures that go above and beyond regulatory requirements.[43]

> *As explained by a security expert:*
>
> Network security (and resilience) requires **thousands of different kinds of controls and techniques**, which must be in place.[44]

For an overview of the main types of measures that operators typically employ to ensure security and resilience, see Table **2**.

41 The European Parliament (2022), Directive (EU) 2022/2555 (link).
42 Based on interviews with security professionals in European telecom operators.
43 Based on interviews with security professionals in European telecom operators.
44 This and following quotes are from our interviews with security experts at several major European telecom operator.

Table 2
Overview of main types of security and resilience measures

	TYPE OF MEASURE	DESCRIPTION
Security	Vulnerability scanning and assessment	• Continuous and automatic vulnerability scanning to detect issues and gaps in defences such that operators can address them before malicious actors exploit them. • Measures are increasingly automated.
	Access management	• Ensures that only the right people can access systems and data, reducing the risk of unauthorised use.
	Threat and intrusions detection measures	• Monitor networks for suspicious activity and alert operators when something unusual or harmful is detected. • Measures are increasingly automated.
	Personnel training	• Employees engage in continuous training on cyber security, data management, and general awareness.
	Procuring secure hardware and software	• Hardware and software providers must meet security standards.
	Physical protection measures	• Includes locks, fences, surveillance, and restricted access to prevent tampering with or damaging critical infrastructure.
Resilience	Business continuity measures (including redundancies of critical systems, power backups, and data backups)	• Ensures that services can continue to run during a disruption, using alternative routes, secure power supply, and data backups.
	Incident management processes	• Well defined and tested processes help operators assess and respond quickly when something goes wrong.
	Disaster recovery plans	• Provide a roadmap for how to restore systems and services after major disruptions.
	Ability to learn from incidents and share intelligence	• Involves analysing what went wrong, improving defences, and working with authorities and peers to prevent future issues.

Note: This is not an exhaustive list of measures but an overview of the main types that we have identified in interviews with security professionals in European telecom operators.
Source: Copenhagen Economics based on interviews with security professionals in European telecom operators and own research.

2.2 SECURITY: SPECIFIC MEASURES IMPLEMENTED BY TELECOM OPERATORS

Security, as defined in this study, refers to measures that prevent attacks, breaches, and other forms of interruptions. For telecom operators, this includes a broad set of activities across infrastructure, systems, and processes. For example, operators must identify potential vulnerabilities, prevent malicious actors from exploiting those vulnerabilities, and detect when there is an error or breach. All of these measures are part of their **overall culture of security**, and all security is integrated within all systems and processes.[45]

As explained by a security expert:

> **Security is in our DNA**. It cannot be implemented as an afterthought – but must be integrated in all systems and processes from the start.

Telecom operators treat security as a top strategic priority and typically structure efforts around dedicated security organisations, led by a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) who is part of top management. These functions oversee multiple specialised teams, including those monitoring activity and threats, managing risks, and responding to incidents.[46]

Operators follow a risk-based approach by continuously assessing where threats may arise and what the consequences could be. Based on these assessments, operators prioritise the areas with the highest risk and potential harm.[47] This approach is reflected in the following activities.

Operators regularly perform **vulnerability scanning and assessment** to identify weak points in systems before they are exploited. Insights from automatic screenings, internal stress-testing, and actual incidents are used to guide operators' efforts.[48,49]

Access management is a key part of preventing unauthorised access to systems and data. It involves controlling who can access what, using tools like identity verification, authentication, and role-based permissions.[50] By limiting access to only those who need it, operators reduce the risk of breaches and protect critical systems from misuse or errors.[51]

Threat and intrusion detection helps operators identify when something is wrong — ideally before it causes damage. Systems are in place to monitor network activity and spot unusual patterns

45 Based on interviews with security professionals in European telecom operators.
46 Based on interviews with security professionals in European telecom operators. See also e.g., Deutsche Telekom (2025, website), Security Management at Deutsche Telekom (link) or Telefonica (2025, website), Cybersecurity (link).
47 Based on interviews with security professionals in European telecom operators.
48 Based on interviews with security professionals in European telecom operators.
49 This is similar to the 'Identify' function in the NIST Cybersecurity Framework. See National Institute of Standards and Technology (2024), The NIST Cybersecurity FrameWork (CSF) 2.0 (link), page 3.
50 This is similar to the 'Protect' function in the NIST Cybersecurity Framework. See National Institute of Standards and Technology (2024), The NIST Cybersecurity FrameWork (CSF) 2.0 (link), page 4.
51 Based on interviews with security professionals in European telecom operators.

or signs that could point to a cyberattack or security breach.[52] Detecting threats early is essential for limiting the impact of incidents and supports a faster and more effective response and recovery.[53] Networks are facing an immense number of potential attacks. For example, Deutsche Telekom's automatic threat detection system evaluates 30,000 to 40,000 attempted attacks per minute and feeds insights from these to a threat intelligence data base.[54]

Operators are increasingly working on automating these security measures, which could have several benefits such as increased speed of response, lower risk of human error, and decreased cost. As Telefónica highlights on their website: "*Through automation, we can reduce response times, minimize human error, and increase efficiency in protecting digital assets*".[55]

Additionally, operators continuously **focus on personnel training** to ensure that employees have the necessary capabilities.[56] This is always needed since a secure network must also be operated in a secure manner.[57]

> *As explained by a security expert:*
> If you build a safe car, you still need to drive it safely. Similar with networks – you need good processes and people to run the network even if it is designed well and built with secure components.

Operators also ensure that their procured **hardware and software** meets latest security requirements.

Additionally, operators ensure **physical protection** of sites and assets using fences, guards, and surveillance. These priorities have gained renewed attention in light of rising geopolitical tensions.[58]

We also note that telecom operators are responsible not only for protecting their own infrastructure from attacks and breaches but also play a key role in **enabling security for end-users** that depend on the network. Telecom networks serve as a door to their end-users, and while they do not control who 'comes through the door' – uses the network – they can detect and respond to suspicious activity by for example identifying and preventing DDoS attacks that targets users.[59]

52 This is similar to the 'Detect function in the NIST Cybersecurity Framework. See National Institute of Standards and Technology (2024), The NIST Cybersecurity FrameWork (CSF) 2.0 (link), page 4.
53 Based on interviews with security professionals in European telecom operators.
54 Deutsche Telekom (2024), Tense cyber situation: Telekom expands protection center (link).
55 Telefónica Tech (2025), Cybersecurity automation with AI to anticipate and neutralize threats (link).
56 See e.g., TDC Net (2025, website), Digital tillid (link).
57 Based on interviews with security professionals in European telecom operators.
58 See e.g., NIS2 Directive (2025, website), Digital Infrastructure Sector (link).
59 Based on interviews with security professionals in European telecom operators. See also Telekom (2024), Tense cyber situation: Telekom expands protection center (link).

Operators have also implemented anti-spoofing[60] and wider anti-fraud solutions on a voluntary basis to ensure consumer safety and trust.[61,62]

In addition, some operators offer security services (e.g. as Managed Security Service Provider) directly to their customers on a commercial basis ('security-as-a-service'), see Box 2.

Box 2 Operators also offer security-as-a-service on commercial terms

Security-as-a-service refers to commercial offerings where telecom operators provide security tools and support to businesses and governments. Services include elements such as threat detection, fraud prevention, and identity protection.

These services are offered on market terms and compensated directly by customers. In contrast, the cost of securing and maintaining the operator's own network is often not visible to end-users and forms part of the baseline cost of running telecom infrastructure.

There are, however, numerous examples of how telecom operators provide security services to companies within critical sectors and to the military.

- For example, Telia provided extra secure services for the NATO summit in Lithuania in 2022. Here they provided multiple points of connection (physical lines and satellite backups), extra firewalls, and specialised anti-DDoS equipment.
- Another example is how Telefónica (through its subsidiary Telefónica Tech) supports governments and companies within critical sectors such as finance, healthcare, and transport. Their services are delivered by specialised cybersecurity teams and 24/7 operations centres, covering areas such as threat detection, data protection, and employee training.
- Deutsche Telekom also offers cybersecurity services through its standalone unit, Telekom Security. Their services are built on 24/7 monitoring, advanced analytics, and expertise developed in protecting Deutsche Telekom's own infrastructure – and are offered to public and private sector clients across Europe.

Source: Telia Company (2024), Annual report 2023, page 17 (link); Telefónica (2024), BBVA signs an agreement with Telefónica Tech to boost cybersecurity (link); Telefónica Tech (2025, website), BBVA Data & AI University: our most ambitious AI and data training project (link); We promote decision-making on Smart Mobility in the United Kingdom (link); Saving Lives with Secure Data (link); Landing in a secure future: shielding critical infrastructure with cyber intelligence (link); and Telekom Security (2025, website), Play it safe with Telekom Security (link).

Operators must stay at the **forefront of innovation** to adapt to the ever-evolving threat landscape. This includes developing new technologies and using state of the art techniques to keep networks secure (and resilient). One example of this is how operators engage in the development of quantum secure communications to prepare for the time when current encryption methods are no longer sufficient, see Box 3.

60 Spoofing is when someone disguises an email address, sender name, phone number, or website URL—often just by changing one letter, symbol, or number—to convince you that you are interacting with a trusted source, see FBI (2025, website), Spoofing and Phishing (link).

61 Orange Developer (2024), New anti-fraud services launched in Spain under the GSMA Open Gateway Initiative (link).

62 Connect Europe (2024), GSMA ETNO position on impersonation fraud in Payment Services Regulation (link).

Box 3 The telecom sector prepares for future threats: Quantum technology

Quantum computing is expected to break current encryption standards, posing a long-term threat to digital security. To stay ahead of this risk, telecom operators are actively involved in developing quantum-secure communication technologies.

- For example, Telefónica contributes to the quantum communications network called 'Madrid Quantum Communication Infrastructure' (MadQCI), which tests quantum key distribution (QKD) technology under real-world conditions as part of preparations for the future European quantum network (EuroQCI). Telefónica's role includes integrating QKD into existing optical networks and helping define operational standards.
- Another example is the EU-funded Nostradamus initiative. As part of a wider consortium, Deutsche Telekom are leading the effort to establish Europe's testing infrastructure for QKD – a technology that enables fundamentally secure data transmission based on the principles of quantum mechanics.
- Similarly in the Petrus Project, Deutsche Telekom is part of a wider consortium that supports and coordinates the deployment of the European Quantum Communication Infrastructure (EuroQCI).
- Also Telecom Italia is actively commercialising QKD via real-world trials in datacentre connections in Athens and submarine cables in Lisbon.

This work supports the creation of a European quantum communication network designed to protect critical infrastructure, including data centres, hospitals, and power grids. It also lays the foundation for future secure satellite communication. These efforts highlight how telecom operators contribute not only to today's security needs but also to the long-term resilience of Europe's digital systems and act as a driver of innovation in the security space.

Source: University of Maryland (2024), Quantum Computing - How it Changes Encryption as We Know It (link); Telefónica (2025, website), Quantum-Safe Networks (link); Telefónica (2025), Telefónica opens a dedicated Centre of Excellence for quantum technologies (link); Telefónica (2024, website), QKD, cryptographic keys and quantum networks (link); Deutsche Telekom (2024), EU launches Nostradamus – prepares Europe for a quantum world (link); Petrus EuroQCI (2025, website), We enable future security - we enable the security of the future (link); Gruppo TIM (2024, website), Sparkle and Telsy Successfully Implement Quantum Security on a High-Capacity Link (link); and Gruppo TIM (2024, website), Telsy implements Quantum Key Distribution with QTI and MEO on terrestrial and submarine fibre optics in the Lisbon metropolitan area (link).

2.3 RESILIENCE: SPECIFIC MEASURES IMPLEMENTED BY TELECOM OPERATORS

Resilience, as defined in this study, refers to measures that minimise the impact for end-users when security is breached, or other events occur that affect the network or systems. Resilience is a top priority for operators and has been expressed as their "licence to operate", since users always notice when services are not available, and it harms the reputation of operators if services break down.

As explained by a security expert:

> When you are a telecom company, resilience is your licence to operate.

For telecom operators, resilience depends both on how networks are built and the ability to respond to incidents.[63] In this section, we group resilience efforts into four main categories:

- Business continuity measures.
- Incident management processes.
- Disaster recovery plans.
- The ability to learn from incidents and share intelligence with government bodies and other operators.

Operators rely on **business continuity measures,** which cover for example redundancies of critical systems, supply chain resilience, and backups.[64] These measures aim at reducing the risk of service interruptions when an incident occurs.

- A key principle in network design is redundancies: operators can build networks with duplicate or alternative components to avoid single points of failure for essential points of access.[65] This can include double or triple connectivity – where there are more than one physical connection (double connectivity) and potentially also satellite backup (triple connectivity) – backup links, and alternative routing paths. If one part fails, another can take over to maintain service continuity. The degree to which these measures are implemented depends on the criticality of the component and the specific end-user. Due to significant costs associated with these measures they are often applied to the most critical access points of the network.
- Power supply is an essential part of the supply chain of telecom networks. To reduce the risk of outages, operators often use emergency power solutions for critical systems. Backup power comes at great financial cost and is usually focused on those parts of the network where it is most critical.[66]
- Operators rely on backups of data, system configurations, and software settings[67] to ensure that critical data is not lost. Operators often spend substantial resources on these backup systems.[68]

As explained by a security expert:

> One of the most important factors for providing sufficient resilience is to have a proven maturity in the backup processes and solutions.

When incidents do occur, operators depend on strong **incident management processes** to handle them. An incident can refer to any disruption, such as a system failure, cyberattack, or other

63 Based on interviews with security professionals in European telecom operators.
64 We have also seen these three concepts used interchangeably but here we distinguish between them.
65 See e.g., Orange Wholesale (2025, website), Operator Secure Connection (OSC) (link).
66 See e.g., Ofcom (2025), Mobile RAN power resilience (link).
67 For a description of backups, see e.g., ZPE (2025, website), Network Resilience vs Redundancy vs Backups (link).
68 Based on interviews with security professionals in European telecom operators.

unexpected events.[69] Responding effectively is an around-the-clock task that involves continuous monitoring, rapid diagnosis, and coordinated action.[70] Operators have dedicated internal response teams — often referred to as Cyber Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) — that manage incidents, classify threats, and coordinate responses with internal teams and external stakeholders.[71]

> *As explained by a security expert:*
> Even the best preventive measures can be abused, so you always need to be able to detect when there is a breach and be able to manage that. We enforce this 24/7.

For more serious or prolonged events, operators activate **disaster recovery plans**. These plans are designed to restore services as quickly as possible and often include predefined procedures, backup infrastructure, and coordination with public entities. Recovery plans are developed in advance and tested regularly to ensure they function in practice.[72,73] Disaster recovery plans are not only relevant within telecom operators, but also across companies and sectors. Some examples include:

- The TEITO exercise in Finland where telecom operators engage in a wider exercise to practice joint action across organisations within government and critical sectors in case of large-scale disruptions to society.[74]
- The 'Bukleap' exercise in Norway organised by Telenor, which brings public authorities, military, and private companies together to practice handling complex cyber-attacks. The goal is to increase collaboration and capacities to solve challenges that can affect critical functions of society.[75]
- How partners from the UP KRITIS initiative (covering critical infrastructure) in Germany conduct IT emergency and crisis exercises in the context of critical infrastructure.[76]

Finally, operators strengthen resilience by **learning from past incidents and sharing intelligence** with peers and authorities. Incidents are reported to regulators, and lessons are integrated into internal routines and systems. Operators also gather insights by running exercises to imitate incidents to test how they are handled.[77] Collaboration across sectors is also increasing. This is for example seen in the Netherlands where KPN is active in the 'CISO Circle of Trust' where 10 major Dutch companies – from technology, finance and energy – corporate to improve their protection against cyber-attacks.[78] At the industry level, GSMA brings together more than 1,000 mobile operators and digital businesses to classify threat actors, share intelligence, and promote best practices.[79]

69 See e.g., ENISA (2024), Telecom security incidents 2022 (link), page 6 for an overview of types of incidents.
70 Based on interviews with security professionals in European telecom operators.
71 See e.g., Deutsche Telekom (2025, website), Introducing Deutsche Telekom CERT (link) or Telefonica (2025, website), Cybersecurity (link).
72 Based on interviews with security professionals in European telecom operators.
73 See e.g., Bridge Connect (2024), How Telecom Operators Handle Disaster Recovery Planning (link).
74 See e.g, Huoltovarmuuskeskus (2024), TIETO24 exercise develops society's preparedness for hybrid threats (link).
75 See e.g., Bukkesprang (2025, website), Bukkesprang 2025 (link).
76 Bundesamt für Sicherheit in der Informationstechnik (2025, website), Drills and exercises (link).
77 Based on interviews with security professionals in European telecom operators.
78 Ministerie van Economische Zaken (2025, website), CISO Circle of Trust (link).
79 GSMA (2024), Establishing MoTIF: The Mobile Threat Intelligence Framework (link).

These shared efforts help identify common vulnerabilities and support collective defences across the sector.

> *As explained by a security expert:*
>
> Resilience means you can react and recover. And, most importantly, you can improve resilience by learning from incidents.

2.4 ENSURING SECURITY AND RESILIENCE COMES AT A SUBSTANTIAL COST TO THE SECTOR

Security and resilience efforts are not isolated functions within the operations of telecom operators but embedded throughout all activities. Operators describe security and resilience efforts as being fundamental to how networks are designed, built, and operated – from procurement and infrastructure design to day-to-day operations.

> *As explained by a security expert:*
>
> Everything we do has a security component to it, so it is impossible to separate the cost of security and resilience from the rest of the business.

Due to the embedded nature of these efforts, it is not possible to cleanly isolate the costs that relate to security and resilience. Additionally, any estimate based on historical data may underestimate costs in a forward-looking context, as it does not account for potential future increases due to evolving threats, technological developments and future policy ambitions.

In any case, research suggests that the costs associated with ensuring security and resilience are significant. For example, relating to security, an estimate from advisory firm Gartner of the costs of providing IT security – only one part of security efforts – finds that IT security spending accounts for 7.3 per cent of total IT spending in the global telecom sector.[80]

The costs associated with providing security and resilience may increase in future, which for example can be seen from NATO's recent commitment for Allies to invest *"up to 1.5% of GDP annually to inter alia protect our critical infrastructure [and] defend our networks"*.[81] This suggests that telecom networks are increasingly viewed as critical to national security, potentially driving higher security and resilience investment requirements in the future.

A recent Ofcom study[82] finds that expanding back-up battery capacity would be extremely costly: upgrading mobile networks in the UK with four-hour battery capacity would cost, depending on assumptions, between GBP 2.2 to 4.4 billion (corresponding to EUR 2.6 to 5.2 billion) as a one-time

[80] Gartner (2024), IT Key Metrics Data 2025: IT Security Measures – Analysis, page 6.
[81] NATO Heads of State and Government (2025), The Hague Summit Declaration, Press Release (link).
[82] Ofcom (2025), Mobile RAN power resilience (link). All estimates are covering the lifetime cost of the assets and are reported in 2024 prices.

investment covering the entire lifetime of the assets.[83] Assuming that such investments are proportional to population size,[84] investing in similar capacity in the EU would cost around EUR 17 to 34 billion as a one-time investment.[85]

[83] Using the average 2024 GBP to EUR exchange rate of 1.1812, see ECB (2025, website), Pound sterling (GBP) (link).

[84] This is a simplified assumption that does not capture differences in for example telecom market structure, geography, and population density.

[85] We scale this by using that fact that in 2024 the EU population (450 million) was 6.5 times larger than the UK population(69 million), see The Worldbank (2025, website), World Development Indicators (link).

CHAPTER 3

POLICYMAKERS HAVE SEVERAL OPPORTUNITIES TO SUPPORT CONTINUED SECURITY AND RESILIENCE

While telecom operators make substantial efforts to secure their networks and maintain resilience, they may face challenges in sustaining and scaling these efforts. As telecom networks provide key infrastructure that support benefits for end-users and wider society, policymakers should consider how to support sufficient funding and resources to overcome challenges and ensure continued security and resilience. Underinvestment in telecom security and resilience could create economy-wide risks that extend far beyond the telecom sector itself.

In this chapter, we describe three key opportunities for policymakers to support continued security and resilience, identified based on operator input: supporting investment in security and resilience, streamlining regulation, and addressing shortages of skilled personnel, see Figure 7.

Figure 7
Policymakers have several opportunities to ensure continued security and resilience

Source: Copenhagen Economics based on interviews with security professionals in European telecom operators.

Support investment in security and resilience

Recent policy reports voice growing concern over the economic sustainability of the telecom sector as some operators struggle to recover the costs of their investments. Financial constraints affecting operators' ability to invest overall could also impact their ability to invest in security and resilience measures.

For example, the Draghi competitiveness report notes that "*in recent years, return on capital has been lower than the weighted average cost of capital*".[86] The European Commission has raised similar concerns, highlighting concerns over EU operators' long-term growth in revenues and degraded access to finance.[87] Similarly, the Letta Single Market report notes that European telecom operators

[86] Draghi (2024), The future of European competitiveness - In-depth analysis and recommendations (link). The report compares the EBIT adjusted return on employed capital with the average weighted cost of capital (WACC).

[87] See e.g., European Commission (2024), White Paper - How to master Europe's digital infrastructure needs? (link).

typically operate at a smaller scale than peers in other global markets, which may limit their ability to spread fixed costs and benefit from economies of scale.[88]

Financial constraints may limit operators' possibilities to strengthen their security and resilience efforts. Some operators suggest that, rather than developing and improving their security and resilience capabilities, they are forced to spend their limited resources on maintaining them.[89]

> *As explained by a security expert:*
>
> The telecom industry is facing financial challenges. This means our priority is to safeguard and continuously enhance the security infrastructure we already have, focusing on efficiency, resilience, and readiness for future growth.

The challenge is exacerbated by accelerating technological development. As both technologies and risks evolve rapidly, legacy systems become harder to protect, and operators must adopt and integrate new solutions to keep pace with innovation. However, it can be costly, time consuming and technically challenging to update or replace legacy systems.[90]

Policymakers should thus consider measures to strengthen the sector's investment capacity and establish regulatory frameworks that support sustained investment in security and resilience.

Recent policy discussions evolve around a call for increased consolidation within the sector to ensure higher investment levels,[91] which is reflected in recent developments at EU level. The Commission's Directorate-General for Competition (DG COMP) is reviewing its merger control guidelines, signalling a shift toward greater emphasis on strategic investment goals and quality outcomes for consumers.[92] This is also reflected in the commission letter from Ursula von der Leyen to the DG COMP Commissioner, Teresa Ribera, which explicitly acknowledges that merger control must evolve to capture needs related to resilience. Security and resilience of telecom networks could reasonably be seen as both strategic objectives and quality factors for end-users. As such, they could play a role in future merger assessments between telecom operators - particularly where robust economic evidence can establish that such improvements are attributable to the merger and result in measurable improvements of security and resilience.

88 See e.g., Letta (2024), Much more than a market - Speed, Security, Solidarity, page 52: "The scale of disparity is stark: an average European operator serves only 5 million subscribers compared to 107 million in the United States and a staggering 467 million in China."

89 Based on interviews with security professionals in European telecom operators.

90 Based on interviews with security professionals in European telecom operators.

91 See e.g., Draghi (2024), The future of European competitiveness - In-depth analysis and recommendations (link); European Commission (2024), White Paper - How to master Europe's digital infrastructure needs? (link); Letta (2024), Much more than a market - Speed, Security, Solidarity, page 52: "enduring fragmentation hinders the scale and growth of pan-European operators, limiting their ability to invest".

92 See e.g., Kluwer Competition Law Blog (2024), The Evolving Role of Non-Price Competitive Parameters in EU Merger Review (link) and Kluwer Competition Law Blog (2024), EVP Ribera's Merger Review Policy Takes Shape (link).

> Your [Teresa Ribera's] work to modernise competition policy will include a review of the Horizontal Merger Control Guidelines. This should give adequate weight to the European economy's more acute needs in respect of resilience, efficiency and innovation, the time horizons and investment intensity of competition in certain strategic sectors, and the changed defence and security environment.

Source: Ursula von der Leyen (2024), Mission letter – Ribera, European Commission (link).

Operators also call for increased public support, or 'risk-sharing' initiatives, to share the costs associated with addressing the complex risk landscape of security and resilience measures. This is sensible where public interests extend beyond commercial interests and additional investments are necessary to achieve certain policy goals such as national security objectives[93] or fraud prevention[94].

Potential policy actions to support continued security and resilience:

- Implement policy frameworks that strengthen the investment capacity of the sector whilst achieving other policy objectives.
- Consider whether and how security and resilience outcomes should be incorporated in merger assessments where they benefit consumers (e.g. through enhanced reliability or fewer outages) and where robust economic evidence can establish that improvements are attributable to consolidation.
- Use public support and 'risk-sharing' initiatives to advance security and resilience investments where public interests extend beyond commercial considerations.

Streamline regulation

Telecom operators face **complex regulatory requirements from overlapping frameworks** relating to security and resilience at EU level, including NIS2, Critical Entities Resilience (CER), and varying transposition of these directives into national legislation, and the Cyber Resilience Act (CRA).

In addition, the interconnected nature of the telecom sector with other sectors creates additional compliance challenges.[95] As the telecom network serves as the backbone for critical sectors, such as healthcare, financial services and energy grids, telecom operators face **regulatory spillover effects**. They must comply not only with telecom-specific regulations but also meet security and resilience standards designed for the sectors they serve. For example, telecom providers serving financial institutions must comply with the Digital Operational Resilience Act (DORA) aimed at the financial sector. This interconnectedness has created a complex compliance matrix where some telecom operators simultaneously answer to communications authorities, financial regulators, health

93 Based on interviews with security professionals in European telecom operators.
94 See e.g., Virgin Media O2 (2025), A 'Victimless crime'? Why fraud policing needs a re-design (link).
95 Based on interviews with security professionals in European telecom operators.

agencies, energy departments, and national security bodies, significantly multiplying their regulatory burden compared to traditional single-sector regulation.[96] See Box **A2** in Appendix A for an overview of selected regulation.

> *As explained by a security expert:*
> The many different regulatory requirements are what we spend most of our time on. The **majority of regulations, guidelines, and directives cover the same things** but have different verifications processes.

These regulatory complexities create **administrative burden**. A study on the economic impact of the NIS2 regulation found that the telecom sector (covering 38 thousand businesses, which is substantially higher than the number of European telecom operators) would spend EUR 900 million more every year to comply with the new regulation. Across all sectors affected by the NIS2, the total cost is estimated to amount to EUR 31.2 billion per year.[97] These costs are in addition to the cost associated with compliance to existing regulation and security and resilience measures already in place. As also noted by the operators, some of these compliance costs will be administrative and unrelated to improving security and resilience.[98]

Operators note that they are often required to prove compliance with overlapping regulations. For instance, one incident may require reporting to several authorities. Operators serving regulated sectors also often face additional audits that cover similar security measures which are already covered by the telecom regulation. This adds compliance and administrative work for operators without meaningful security improvements.[99]

> *As explained by a security expert:*
> We face a lot of regulation and spend a lot of time and money on proving and administering compliance. **If we were facing less extensive regulation and administrative measures, we could spend more time on real security measures instead of on compliance**. That is the one thing, I would do differently.

Telecom networks are inherently interconnected not only across sectors but also internationally through cross-border interconnects, roaming, subsea cables, and shared services. This means that failures or cyberattacks in one network can create cascading risks that rapidly spread to other countries and sectors. This interconnectedness means that modern network resilience increasingly depends on dynamic response capabilities, i.e. the ability to reroute traffic and shift operations during

96 Based on interviews with security professionals in European telecom operators.

97 Frontier Economics (2023), Assessing the Economic Impact of EU Initiatives on Cybersecurity (link), page20. Note that their definition of the telecommunication sector ("Providers of electronic communications networks or of publicly available electronic communications services: Telecom") goes beyond core telecom operators and is thus wider than what we use in this report.

98 Based on interviews with security professionals in European telecom operators.

99 Based on interviews with security professionals in European telecom operators and Arthur D. Little (2025), A simplification agenda for European Telecoms, pages 24-26

outages or cyberattacks. However, nationally imposed security requirements, covering asset localisation within national borders, restrictions on remote access, and national security clearance may create protective silos around national networks, which can hinder operators' ability to effectively collaborate cross-border and respond to cascading threats.[100]

There are also examples of restrictions on certain vendors which limit operator options, which may impact cost and innovation. Such challenges are, however, not a focus of this study.

Potential policy actions to support continued security and resilience:

- Streamline existing regulation and international standards to address overlaps between different requirements applying to the telecom sector directly and via the sectors they serve, e.g.:
    - Assess overlapping requirements between sector-specific regulations (e.g. DORA) and horizontal frameworks (e.g. NIS2) with a view to removing redundant requirements.
    - Review and align definitions, thresholds and procedures across regulations, where possible, to streamline reporting requirements and establish a single-entry point for reporting.
- Review national security frameworks to ensure that they support dynamic, cross-border network resilience

Address skill shortages

Ensuring secure and resilient telecom networks requires highly specialised experts. However, telecom operators face increasing difficulty in attracting and retaining qualified staff.

> *As explained by a security expert:*
> Working in security requires a certain skill set. **There is always a shortage of those skills, and it is a struggle to find the right candidates available on the market**.

The challenge reflects a broader shortage of cybersecurity professionals across Europe. OECD estimates that the region faces a shortfall of around 300,000 skilled workers in the field.[101] More than half of companies seeking to recruit cybersecurity professionals report difficulties in filling roles, primarily due to a lack of qualified candidates.[102] This shortage limits operators' capacity to scale their security efforts and maintain 24/7 coverage, and it increases dependence on a small pool of in-demand experts. It may also contribute to increasing labour costs,[103] which increases the operators' total costs of providing security and resilience.

[100] Based on interviews with security professionals in European telecom operators and Arthur D. Little (2025), A simplification agenda for European Telecoms, pages 24-26.

[101] OECD (2024), Building a Skilled Cyber Security Workforce in Europe (link).

[102] EU Digital Skills & Jobs (2024), EU faces growing cybersecurity skills gap, new Eurobarometer reveals (link).

[103] If the demand of skilled labour is higher than the supply, operators might need to increase salaries to attract the needed talent.

The skill shortage is widely recognised, and several initiatives have been started to alleviate the issue. One example is the EU led 'Cyber skills academy' aiming to address the skill shortage by "*bringing together and improving the coordination of existing training, upskilling and reskilling initiatives for cybersecurity professionals*."[104] Both businesses and higher education institutions have pledged to contribute with different training initiatives. Some of these are led by operators who aim to train cybersecurity professionals to address the shortage.[105]

Potential policy actions to support continued security and resilience:[106]

- Develop a future-proof EU cybersecurity skill strategy.

[104] EU Digital Skills & Jobs (2025, website), Cybersecurity Skills Academy (link).

[105] See e.g., EU Digital Skills & Jobs (2025), Orange commits to closing the cybersecurity skills gap with new pledge for Cybersecurity Skills Academy (link).

[106] See Access Partnership (2024), Cybersecurity skills in the EU: A new dawn? (link).

REFERENCES

Access Partnership (2024), Cybersecurity skills in the EU: A new dawn?, Available here. Accessed 26 June 2025.

AP (2025), At least 11 Baltic cables have been damaged in 15 months, prompting NATO to up its guard, Available here. Accessed 26 June 2025.

Arthur D. Little (2025), A simplification agenda for European Telecoms. Available here. Accessed 28 July 2025.

Berec (2023), BEREC Report on the Current Cybersecurity Challenges and Dependencies in Electronic Communication Networks, Available here. Accessed 26 June 2025.

BEREC (2025, website), What are Very High Capacity Networks?, Available here. Accessed 27 June 2025.

Berlingske (2024), Nu afslører TDC årsagen til det store mobilnedbrud – og det burde ikke kunne ske, Available here. Accessed 26 June 2025.

Bridge Connect (2024), How Telecom Operators Handle Disaster Recovery Planning, Available here. Accessed 26 June 2025.

Briglauer, Krämer, and Palan (2023), Socioeconomic benefits of high-speed broadband availability and service adoption: A survey, Available here. Accessed 26 June 2025.

Bukkesprang (2025, website), Bukkesprang 2025, Available here. Accessed 18 September 2025.

Bundesamt für Sicherheit in der Informationstechnik (2025, website), Drills and exercises, Available here. Accessed 26 June 2025.

Bundesgesetzblatt (2015), Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)*, Available here. Accessed 26 June 2025.

Center for Cybersikkerhed (2019), Cybertruslen mod telesektoren, Available here. Accessed 26 June 2025.

Center for Cybersikkerhed (2021), Truslen fra destruktive cyberangreb, Available here. Accessed 26 June 2025.

Center for Cybersikkerhed (2022), Cybertruslen mod telesektoren.

Center for Cybersikkerhed (2025), Cybertruslen mod telesektoren, Available here. Accessed 26 June 2025.

Cloudflare (2025, website), What is a DDoS attack?, Available here. Accessed 26 June 2025.

Connect Europe (2024), GSMA ETNO position on impersonation fraud in Payment Services Regulation, Available here. Accessed 26 June 2025.

Cyberscoop (2022), String of attacks on French telecom infrastructure preceded April attack on fiber optic cables, Available here. Accessed 26 June 2025.

Cybersecurity Dive (2024), Telecom, media and tech companies are cyber defense standouts: Moody's, Available here. Accessed 26 June 2025.

Cybersecurity & Infrastructure Security Agency (2025, website), Communications Sector, Available here. Accessed 26 June 2025.

Deloitte (2016), The economic impact of disruptions to internet connectivity.

Deutsche Telekom (2024), EU launches Nostradamus – prepares Europe for a quantum world, Available here. Accessed 26 June 2025.

Deutsche Telekom (2024), Tense cyber situation: Telekom expands protection center, Available here. Accessed 26 June 2025.

Deutsche Telekom (2025, website), Introducing Deutsche Telekom CERT, Available here. Accessed 26 June 2025.

Deutsche Telekom (2025, website), Security Management at Deutsche Telekom, Available here. Accessed 31 July 2025.

DR (2024), Massivt nedbrud hos TDC skabte 112-kaos: Nu lover Teleindustrien forbedringer, Available here. Accessed 31 July 2025.

Draghi (2024), The future of European competitiveness - In-depth analysis and recommendations, Available here. Accessed 26 June 2025.

ECB (2025, website), Pound sterling (GBP), Available here. Accessed 31 July 2025.

ENISA (2020), Power Sector Dependency on Time Service, Available here. Accessed 26 June 2025.

ENISA (2023), Telecom security incidents 2022, Available here. Accessed 31 July 2025.

ENISA (2023), ENISA Threat Landscape 2023, Available here. Accessed 27 June 2025.

ENISA (2023), Subsea Cables – what is at stake?, Available here. Accessed 26 June 2025.

ENISA (2024), 2024 Report on the State of the Cybersecurity in the Union, Available here. Accessed 26 June 2025.

ENISA (2024), Telecom security incidents 2022, Available here. Accessed 26 June 2025.

ENISA (2024), ENISA Threat Landscape 2024, Available here. Accessed 27 June 2025.

ENISA (2025), Telecom security incidents 2024, Available here. Accessed 31 July 2025.

ENISA (2025, website), Glossary of Terms, Available here. Accessed 31 July 2025.

EU Digital Skills & Jobs (2024), EU faces growing cybersecurity skills gap, new Eurobarometer reveals, Available here. Accessed 26 June 2025.

EU Digital Skills & Jobs (2025), Orange commits to closing the cybersecurity skills gap with new pledge for Cybersecurity Skills Academy, Available here. Accessed 26 June 2025.

European Commission (2024), Protecting competition in a changing world, Evidence on the evolution of competition in the EU during the past 25 years, Available here. Accessed 26 June 2025.

European Commission (2024), White Paper - How to master Europe's digital infrastructure needs?, Available here. Accessed 26 June 2025.

European Commission (2025), Commission calls on 19 Member states to fully transpose the NIS2 Directive, Available here. Accessed 26 June 2025.

European Insurance and Occupational Pensions Authority (2025, website), Digital Operational Resilience Act (DORA), Available here. Accessed 26 June 2025.

European Parliament (2019), Cybersecurity Act (Directive 2018/1972), Available here. Accessed 31 July 2025.

European Parliament (2022), CER Directive (Directive 2022/2557), Available here. Accessed 31 July 2025.

European Parliament (2022), NIS 2 Directive (Directive 2022/2555), Available here. Accessed 31 July 2025.

European Parliament (2024), Cyber Resilience Act (Regulation 2024/2847), Available here. Accessed 26 June 2025.

Eurostat (2025), Digitalisation in Europe – 2025 edition, Available here. Accessed 26 June 2025.

Eurostat (2025, website), Broadband internet coverage by technology (online data code: isoc_cbt), Available here. Accessed 26 June 2025.

Eurostat (2025, website), Individuals - frequency of internet use (online data code: isoc_ci_ifp_fu), Available here. Accessed 26 June 2025.

Eurostat (2025, website), Internet access by size class of enterprise (online data code: isoc_ci_in_es), Available here. Accessed 26 June 2025.

Eurostat (2025, website), Meetings via the internet by size class of enterprise (online data code: isoc_ci_mvis), Available here. Accessed 26 June 2025.

Eurostat (2025, website), Population on 1 January (online data code: tps00001), Available here. Accessed 26 June 2025.

Eurostat (2025, website), Use of electronic identification (eID) (online data code: isoc_eid_ieid), Available here. Accessed 26 June 2025.

Eurostat (2025, website), Value of e-commerce sales by NACE Rev. 2 activity (online data code: isoc_ec_evaln2), Available here. Accessed 26 June 2025.

Eurostat (website, 2025), E-government activities of individuals via websites (Online data code: isoc_ciegi_ac), Available here. Accessed 26 June 2025.

FBI (2025, website), Spoofing and Phishing, Available here. Accessed 26 June 2025.

Finextra (2025), Spanish mobile networks go dark, Available here. Accessed 31 July 2025.

Forbes (2022), How to Guard Against The Cost Of Unplanned Downtime And Network Outages, Available here. Accessed 26 June 2025.

Frontier Economics (2023), Assessing the Economic Impact of EU Initiatives on Cybersecurity, Available here. Accessed 31 July 2025.

Gartner (2024), IT Key Metrics Data 2025: IT Security Measures – Analysis.

Genakos, Valletti, and Verboven (2018), Evaluating market consolidation in mobile communications. Economic Policy, 33(93), 45-100, Available here. Accessed 26 June 2025.

Giroud et al. (2021), Propagation and Amplification of Local Productivity Spillovers, Available here. Accessed 31 July 2025.

Gruppo TIM (2024, website), Sparkle and Telsy Successfully Implement Quantum Security on a High-Capacity Link, Available here. Accessed 31 July 2025.

Gruppo TIM (2024, website), Telsy implements Quantum Key Distribution with QTI and MEO on terrestrial and submarine fibre optics in the Lisbon metropolitan area, Available here. Accessed 31 July 2025.

GSMA (2024), Establishing MoTIF: The Mobile Threat Intelligence Framework, Available here. Accessed 26 June 2025.

Huoltovarmuuskeskus (2024), TIETO24 exercise develops society's preparedness for hybrid threats, Available here. Accessed 26 June 2025.

ISO (2025, website), ISO/IEC 27001:2022, Available here. Accessed 26 June 2025.

ITU (2017), ICT for ENERGY – Telecom and Energy Working Together for Sustainable Development, Available here. Accessed 31 July 2025.

Kluwer Competition Law Blog (2024), EVP Ribera's Merger Review Policy Takes Shape, Available here. Accessed 26 June 2025.

Kluwer Competition Law Blog (2024), The Evolving Role of Non-Price Competitive Parameters in EU Merger Review, Available here. Accessed 26 June 2025.

Kongaut and Bohlin (2017), Impact of broadband speed on economic outputs: An empirical study of OECD countries, Available here. Accessed 31 July 2025.

Letta (2024), Much more than a market - Speed, Security, Solidarity.

Ministerie van Economische Zaken (2025, website), CISO Circle of Trust, Available here. Accessed 26 June 2025.

National Institute of Standards and Technology (2024), The NIST Cybersecurity Framework (CSF) 2.0, Available here. Accessed 26 June 2025.

NATO Heads of State and Government (2025), The Hague Summit Declaration, Press Release, Available here. Accessed 31 July 2025.

NIS Cooperation Group (2023), EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors, Available here. Accessed 26 June 2025.

NIS Cooperation Group (2024), Cybersecurity and resiliency of Europe's communications infrastructures and networks, Available here. Accessed 26 June 2025.

NIS2 Directive (2025, website), Digital Infrastructure Sector, Available here. Accessed 26 June 2025.

OECD (2024), Building a Skilled Cyber Security Workforce in Europe, Available here. Accessed 26 June 2025.

Ofcom (2024), Statement on Network and Service Resilience Guidance, Available here. Accessed 31 July 2025.

Ofcom (2025), Mobile RAN power resilience, Available here. Accessed 29 July 2025.

Okoro et al. (2024), Digital communication and U.S. economic growth: a comprehensive exploration of technology's impact on economic advancement, Available here. Accessed 26 June 2025.

Openreach (2025), Storm Eowyn, Available here. Accessed 1 August 2025.

Orange Developer (2024), New anti-fraud services launched in Spain under the GSMA Open Gateway Initiative, Available here. Accessed 26 June 2025.

Orange Wholesale (2025, website), Operator Secure Connection (OSC), Available here. Accessed 26 June 2025.

Padilla (2024) Do Four-to-Three Mobile Mergers Harm Consumers? A Deep-Dive into the UK Market, Available here. Accessed 27 June 2025.

Parametrix (2024), CrowdStrike's Impact on the Fortune 500 – An Impact Analysis, Available here. Accessed 1 September 2025.

Petrus EuroQCI (2025, website), We enable future security - we enable the security of the future, Available here. Accessed 31 July 2025.

Pingdom (2023), Average Cost of Downtime per Industry, Available here. Accessed 26 June 2025.

Ponemon Institute (2016), Cost of Data Center Outages.

Rabobank (2025), Facts and lessons learned from the Iberian blackout, Available here. Accessed 31 July 2025.

Reuters (2020), Dutch telecommunications towers damaged by 5G protestors: Telegraaf, Available here. Accessed 26 June 2025.

SVT (2025), Granskning: Angrepp mot 30-tal telemaster – utreds som sabotage, Available here. Accessed 31 July 2025.

TDC Net (2025, website), Digital tillid, Available here. Accessed 26 June 2025.

Telecom Advisory Services (2020), Assessing the Economic Potential of 10G Networks, Available here. Accessed 26 June 2025.

Telefónica (2024), BBVA signs an agreement with Telefónica Tech to boost cybersecurity, Available here. Accessed 26 June 2025.

Telefónica (2024, website), QKD, cryptographic keys and quantum networks, Available here. Accessed 31 July 2025.

Telefónica (2025), Telefónica opens a dedicated Centre of Excellence for quantum technologies, Available here. Accessed 26 June 2025.

Telefónica (2025, website), Cybersecurity, Available here. Accessed 31 July 2025.

Telefónica (2025, website), Quantum-Safe Networks, Available here. Accessed 26 June 2025.

Telefónica Tech (2025), Cybersecurity automation with AI to anticipate and neutralize threats, Available here. Accessed 26 June 2025.

Telefónica Tech (2025, website), BBVA Data & AI University: our most ambitious AI and data training project, Available here. Accessed 26 June 2025.

Telefónica Tech (2025, website), Landing in a secure future: shielding critical infrastructure with cyber intelligence, Available here. Accessed 26 June 2025

Telefónica Tech (2025, website), Saving Lives with Secure Data, Available here. Accessed 26 June 2025.

Telefónica Tech (2025, website), We promote decision-making on Smart Mobility in the United Kingdom, Available here. Accessed 26 June 2025.

Telekom Security (2025, website), Play it safe with Telekom Security, Available here. Accessed 31 July 2025.

Telia Company (2024), Annual report 2023, page 17, Available here. Accessed 26 June 2025.

The Guardian (2025), 'Shadow fleets' and subaquatic sabotage: are Europe's undersea internet cables under attack?, Available here. Accessed 26 June 2025.

The Irish Times (2025), Plan under way to protect telecoms network from extreme weather, Available here. Accessed 26 June 2025.

The Worldbank (2025, website), World Development Indicators, Available here. Accessed 1 August 2025.

University of Maryland (2024), Quantum Computing - How it Changes Encryption as We Know It, Available here. Accessed 26 June 2025.

Ursula von der Leyen (2024), Mission letter – Ribera, European Commission, Available here. Accessed 4 September 2025.

World Economic Forum (2019), Digital technology can cut global emissions by 15%. Here's how, Available here. Accessed 31 July 2025.

World Economic Forum (2025), Global Cybersecurity Outlook 2025, Available here. Accessed 31 July 2025.

ZPE (2025, website), Network Resilience vs Redundancy vs Backups, Available here. Accessed 26 June 2025.

APPENDIX A

Box A1 Different definitions of security and resilience

To our knowledge, there are no widely agreed definitions of security and resilience in relation to telecom networks. Definitions vary across regulatory bodies, frameworks and regulations, as outlined below.

ENISA defines security incidents and resilience in the following way:

- "***Security incident**: An occurrence that harms integrity, accessibility, confidentiality or authenticity of a computer (or other device) or a network.*"
- "***Resilience**: The ability to recover from faults in addition to the ability to provide and maintain.*"

Different EU regulations, national regulators, and international standards cover the same overarching points, while nuances vary across definitions:

- The EU Cybersecurity Act defines **cybersecurity** as: "*the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats*".
- The EU NIS2 directive also use the CIA triad (confidentiality, integrity, and availability) in the definition of '**security of network and information systems**': "*[…] the ability of [a system] to resist […] any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered*".
- Similarly, the ISO27001 standard highlights confidentiality, integrity, and availability as the three principles of **information security**.
- The EU CER directive defines **resilience** as: "*a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident*"
- The British telecom regulator, Ofcom, interprets **resilience** as: "*the ability of an organisation, resource, or structure to be resistant to a range of known and future internal and external threats, to withstand the effects of a partial loss or degradation of platform, system, or service, to recover and resume service with the minimum reasonable loss of performance, and adopt lessons learnt from any incidents.*"

There are certain overlaps between security and resilience, where resilience is often interpreted as a more holistic term that includes security measures. For simplicity in this study, we carve out the security elements (prevent, protect, etc.) from resilience and treat them as two distinct concepts.

Source: ENISA (2025, website), Glossary of Terms (link); European Parliament (2019), Cybersecurity Act (Directive 2018/1972) (link); European Parliament (2022), NIS 2 Directive (Directive 2022/2555) (link); ISO (2025, website), ISO/IEC 27001:2022 (link); European Parliament (2022), CER Directive (Directive 2022/2557) (link); Ofcom (2024), Statement on Network and Service Resilience Guidance (link); and Based on interviews with security professionals in European telecom operators.

Box A2 Telecom operators face multiple security and resilience regulations

Telecom operators are subject to a range of regulatory requirements alongside voluntary standards such as ISO 27001. These include EU-level rules like NIS2, the Critical Entities Resilience (CER) Directive, and the Cyber Resilience Act (CRA), as well as national legislation. In addition, operators are often indirectly covered by sector-specific regulations — for example, financial sector rules such as DORA — when providing services to regulated customers. Below we present a set of selected regulations that affects operators but note that it is not an exhaustive list.

- **The NIS2 Directive** builds on the original EU-wide cybersecurity legislation (NIS) by responding to the growing threat landscape. It introduces stricter security requirements, streamlines reporting, and expands the scope to cover more sectors — including telecom operators, who are now classified as essential entities. As a result, telecom operators face increased obligations related to incident response, supply chain risk, and physical security, as well as heightened regulatory oversight. Note that at the time of writing, NIS2 was not fully implemented across all member states.
- **The CER Directive** aims to strengthen resilience frameworks by requiring providers of essential services to ensure their ability to withstand all types of disruptions: natural, intentional, or accidental. It builds upon the previous Critical Infrastructure Directive of 2008 by expanding coverage to 11 sectors.
- **The CRA** introduces EU-wide cybersecurity requirements for hardware and software products. The CRA entered into force in December 2024, but the main obligations introduced by the act will only apply from December 2027. While the regulation primarily targets manufacturers, it also affects telecom operators, who rely on a wide range of digital products in their networks. As buyers of equipment, operators must ensure that the components they procure comply with CRA requirements, adding new obligations related to supply chain security.
- **National regulation,** such as IT-Sicherheitsgesetz (IT Security Act) in Germany, aims to strengthen the protection of critical infrastructure by setting mandatory cybersecurity requirements. For telecom operators, this means regular audits, incident reporting obligations, and compliance with minimum technical and organisational standards. Note that national regulation – and the related requirements – can differ substantially across countries.
- Under **DORA**, telecom operators are increasingly subject to scrutiny as critical third-party ICT providers to financial institutions. Designated entities must meet stringent requirements on ICT risk management, operational resilience testing, incident reporting, and third-party oversight.

Source: European Parliament (2022), NIS 2 Directive (Directive 2022/2555) (link); NIS2 Directive (2025, website), Digital Infrastructure Sector (link); Eurpopean Commission (2025), Commission calls on 19 Member states to fully transpose the NIS2 Directive (link); European Parliament (2022), CRE Directive (Directive 2022/2557) (link); European Parliament (2024), Cyber Resilience Act (Regulation 2024/2847) (link); Bundesgesetzblatt (2015), Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)* (link); European Insurance and Occupational Pensions Authority (2025, website), Digital Operational Resilience Act (DORA) (link).