Copenhagen Economics

SUPPORTING RESILIENT TELECOM NETWORKS IN DENMARK

Assessment of investment needs and policy options

Report commissioned by TDC Net
July 2026

Preface

Over the past few decades, EU telecom policy has been driven primarily by objectives of promoting competition, ensuring broad coverage, and delivering affordable connectivity for consumers and businesses. This approach has helped deliver high-quality and affordable telecom services across Europe.

In recent years, however, policy priorities have begun to shift. Today, telecom networks underpin essential functions, ranging from everyday communications to critical public and private services. At the same time, various risks have emerged that increasingly threaten the functioning of telecom infrastructure, such as cyberattacks, physical sabotage, and power blackouts.

As a result, the resilience[1] of telecom networks has moved to the forefront of the policy agenda. Against this backdrop, it is timely to revisit the policy framework to ensure that it supports the investments needed to deliver secure and resilient telecom infrastructure.

TDC Net has commissioned Copenhagen Economics to assess how Denmark can ensure sufficient investment in resilient telecom infrastructure in the years ahead. In this report, we first examine why there is an increasing need for investment in resilient telecom networks. Second, we develop forward-looking scenarios for the level of resilience investments that may be necessary. Finally, we consider how the policy framework could be adapted to ensure that telecom operators are able to deliver the investments needed to meet society's growing resilience requirements.

1) In this report, we use the term 'resilience' to cover both security and resilience measures, that is, measures to avoid and prevent attacks, breaches, and interruptions, as well as measures to avoid or minimise any impact on end-users when an incident occurs.

Executive summary (1/3)

There is an increasing need for resilience investments in telecom networks

Several parallel developments in recent years have increased the need for investment in the resilience of Denmark's telecom networks.

First, **digital dependency has increased**, as households, businesses, and public authorities now rely on connectivity for almost all essential services, daily operations, and communication. TDC Net plays a particularly important role in Denmark due to the uniquely broad scope of its network.

Second, **the threat landscape has expanded**, and telecom infrastructure is exposed to a broader mix of threats. In Ukraine, Russia's war has involved large-scale attacks on communications infrastructure. In 2025, a power blackout across the Iberian Peninsula disrupted connectivity services for millions of people for several hours. Events such as these illustrate that networks are being tested under increasingly severe conditions.

Together, these developments mean that **regulatory and societal expectations for resilience are rising.** New and more stringent resilience requirements may be introduced in years ahead. At the same time, citizens, businesses, and public authorities increasingly take for granted that telecom operators do whatever they can to ensure secure, reliable connectivity.

As a result, telecom operators will need to continue, and in some cases accelerate, their resilience-related investments.

TDC Net could face resilience investments of up to DKK 4.7 billion between 2026 and 2030

We estimate that TDC Net could face resilience-related investments of up to DKK 4.7 billion between 2026 and 2030, depending on future resilience requirements and the underlying assessment of risks.

To assess the potential investment need, we have developed three scenarios:

- *Preparedness Level One: fit for current risk landscape:* Maintain and strengthen the existing resilience foundation, based on commercial interests and compliance with current regulatory requirements.
- *Preparedness Level Two: fit for elevated risk landscape:* Upgrade existing capabilities to address increasing regulatory requirements and societal expectations.
- *Preparedness Level Three: fit for extensively elevated risk landscape – crisis ready:* Prepare for unprecedented but plausible events, including conflict scenarios that affect Denmark.

There is considerable uncertainty regarding the investments required under each scenario, as future threats, disruptions, and regulatory requirements are inherently difficult to predict.

Nevertheless, we have identified a non-exhaustive list of potential resilience investments and developed cost estimates based on input from TDC Net.

Our analysis indicates that resilience-related investments could amount to:

- approximately DKK 2.1–2.6 billion in the Preparedness Level One: fit for current risk landscape resilience scenario;
- approximately DKK 2.7–3.6 billion in the Preparedness Level Two: fit for elevated risk landscape resilience scenario; and
- approximately DKK 3.4-4.7 billion in the Preparedness Level Three: fit for extensively elevated risk landscape – crisis ready resilience scenario.

Overall, resilience-related investments in 2030 could correspond to around 40 per cent of TDC Net's total investment level in 2025.

Executive summary (2/3)

The current policy framework was not designed to support resilience investments

Markets do not always deliver outcomes that are optimal for society. In the case of resilience investments, we identify **three market failures that mean telecom operators will not invest at the socially optimal level**:

- *A public good with positive externalities:* Operators cannot capture the full societal value of resilience. More resilient telecom networks strengthen the security of Danish society as a whole by protecting critical communications infrastructure and making Denmark a less attractive target for hybrid attacks. However, because these benefits accrue broadly across many parties, operators cannot fully monetise the value they create, so they have weaker incentives to invest than would be optimal from a societal perspective.
- *Quality opacity:* Customers cannot easily observe resilience. Most customers choose providers based on factors such as price, speed, and data allowances rather than network resilience. As a result, operators have limited ability to monetise resilience beyond minimum requirements, reducing incentives to invest in higher levels of resilience.
- *Coordination failures:* No single actor has the full picture. Authorities have a broad view of societal risks and security priorities, while operators have detailed knowledge of technical solutions and investment costs. Without effective coordination, some important resilience measures may not be implemented, and investments may not be directed towards the areas that generate the greatest reduction in societal risk.

Taken together, these market failures imply that resilience investments will diverge from the socially optimal level.

Imposing investment obligations alone may not deliver the desired outcomes. While it may be tempting for policymakers to address resilience gaps by directly imposing investment obligations, such an approach may not be effective for three main reasons.

First, ability to absorb costs. Operators would end up bearing most of the costs, as it is difficult to pass on investment costs in competitive markets, as well as in markets subject to price regulation. Danish operators are already financially strained, and imposing further investment obligations would squeeze resources and potentially crowd out other necessary investments.

Second, competitive distortions. If obligations are applied asymmetrically across operators, with some operators facing more obligations than others, they may distort competition to the detriment of consumers.

Third, reduced effectiveness through prescriptive design. Highly detailed requirements on specific assets or technologies can shift incentives towards compliance rather than outcomes, reducing flexibility and limiting operators' ability to optimise network-wide resilience.

Taken together, these factors suggest that investment obligations alone may be insufficient to deliver efficient and effective resilience outcomes.

More broadly, **the current policy framework should be revisited to ensure it reflects the policy priorities of today.** Sector-specific regulation affecting the telecom industry has been developed over time, historically focused on objectives such as competition, coverage, and affordability. For example, significant market power (SMP) regulation was primarily designed to address market power (in fixed networks, such as fibre) by promoting competition and keeping prices low.

While security and resilience have become increasingly important policy priorities, the current framework was not designed with these objectives at its core. There are no regulatory tools which directly address the identified market failures. Accordingly, it is timely to revisit the policy framework to ensure it is aligned with today's policy priorities.

Executive summary (3/3)

Effective resilience requires authorities and operators to work together. A more collaborative approach between authorities and operators can help reduce coordination failures by sharing data, scenarios, and technical assessments, and by aligning expectations on required resilience levels, costs, and priorities. It can thereby operationalise the sector's 'societal contract' (in Danish, samfundskontrakt), ensuring clear shared objectives, principles for cost recovery, and policy priorities.

While a collaborative effort is important to identify the right level and mix of resilience investments, it does not address the question of who pays.

Any investment obligations should be accompanied by financing mechanisms. Where strategic societal objectives go beyond commercial incentives, financing mechanisms should be in place. We identify three broad options:

- **Measures to strengthen operators' investment capacity:** Adjustments to the regulatory framework could enable operators to finance a greater share of resilience investments from their own balance sheets. With such an approach, accountability and transparency would be key, meaning that any additional flexibility would have to be matched by increased accountability, e.g. clear resilience commitments and additional reporting to document that extra financial capacity is actually being used to strengthen resilience.

  One way of strengthening operators' investment capacity would be to loosen or remove regulatory price caps which currently apply to operators with local market power, such as TDC Net or Norlys. This approach could be implemented quickly and cost-effectively, although it has two main weaknesses (i) that customers in regulated SMP areas would likely bear the cost of resilience investments through higher retail prices, even though these investments benefit national telecom infrastructure more broadly, and (ii) that operators' ability to finance resilience investments would be uneven, as non SMP operators would only benefit indirectly, and only in some market contexts, from the increased pricing flexibility granted to SMP operators.

  A second way of strengthening operators' investment capacity would be to support economies of scale, for example through allowing mergers or network-sharing agreements that clearly enhance resilience incentives without disproportionately harming competition. This can lower unit costs, thus making more investments financially viable and/or freeing up resources. However, such an approach must be designed and implemented carefully to avoid the harm from reduced competition exceeding the resilience upside.
- **A compensation fund supported by a special levy on telecom services:** A dedicated fee (e.g. 10%) on telecom services could be used to finance a compensation fund for resilience investments. This approach would link costs directly to users of telecom services and could provide a stable funding base. However, it could also face political resistance (as with any new tax) and could generate administrative burden associated with managing the fund (e.g. prioritising funds between different applications, managing complaints, etc.). Thus, it is difficult to ensure that funding is allocated fairly.
- **Direct public funding (state aid):** Public grants can be used to finance specific resilience investments, such as hardening critical sites, adding backup power, or upgrading key network infrastructure. This approach allows funding to be targeted and linked to measurable projects, but it must compete with other public spending (meaning that there may be little political will to dedicate funding), can be subject to stop-start budget cycles, and leads to added complexity due to state aid rules.

Table of contents

CHAPTER 1

THERE IS AN INCREASING NEED FOR RESILIENCE INVESTMENTS IN TELECOM NETWORKS

Chapter 1 – Structure

1.1 Digital dependency has increased	• Resilient telecom networks play a crucial role in Danish society. • TDC Net plays a particularly important role.
1.2 The threat landscape has expanded	• Telecom networks are exposed to a broad and evolving set of threats. • Real-world examples illustrate that networks are increasingly being put to the test. • The threat picture has changed in Denmark.
1.3 Regulatory and societal expectations for resilience are rising	• The current policy framework for the telecom sector covers multiple areas, including resilience. • New resilience regulations will likely be implemented. • Further investment will be needed to increase the resilience of the telecom networks.

Modern and sustainable **digital infrastructures** for connectivity and computing **are critical enablers for digitalisation** and therefore both for the industrial competitiveness and for society to benefit fully from digital services. For that reason, high-quality, **secure and resilient connectivity** for everybody and everywhere in the Union **is needed**, […]

European Commission (2026). Proposal for a Regulation for the Digital Networks Act (DNA). Link.

Digital dependency has increased

1.1

Resilient telecom networks play a crucial role in Danish society

The dependency on reliable telecom connectivity is rising as citizens, businesses, and governments digitise. As recognised by the European Commission in its proposal for the Digital Network Act, secure and resilient telecom infrastructure is needed, as it is a critical enabler of digitalisation for the benefit of society. Similarly, NATO notes that critical infrastructure supports core government functions, everyday services for households and businesses, and, in many cases, security and defence objectives.[1]

"Our economies and our democratic societies rely on critical infrastructure, which provides essential services to our citizens and underpins our economies. Military forces also rely to a great degree on public and private civilian infrastructure to be able to fulfil their tasks."

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.

In a digital nation like Denmark, dependence on digital services is substantial. For example, 78 per cent of Danish businesses engaged in online meetings in 2025, compared with an EU average of 53 per cent, see Figure 1 in Box 1. Similarly, 98 per cent of Danish citizens used a website or an app of public authorities, compared with 69 per cent among all EU citizens, see Figure 2 in Box 1.

As key services move to online and cloud-based platforms, disruptions in telecom networks increasingly have wide-ranging consequences, with large parts of society and the economy at risk of grinding to a halt when connectivity fails.

The dependency on telecom networks is also highlighted in the Draghi report, where high-speed broadband networks and related systems are one of the three key areas of digitalisation and advanced technologies in which policies and initiatives should be prioritised.[2]

Consequently, telecom networks are evolving from a support function into a core enabler of economic activity, social participation and public safety.

TDC Net plays a particularly important role

In Denmark, TDC Net plays a particularly important role for two reasons.

First, TDC Net operates one of Denmark's most extensive backbone networks, i.e. behind-the-scenes infrastructure supporting many other operators' networks. TDC Net's infrastructure comprises several layers and spans the entire country. This infrastructure supports high traffic volumes and enables both national and international connectivity. In Denmark, only GlobalConnect has a comparable backbone network. See Table 1 in Box 2 for more details about TDC Net's backbone network.[3]

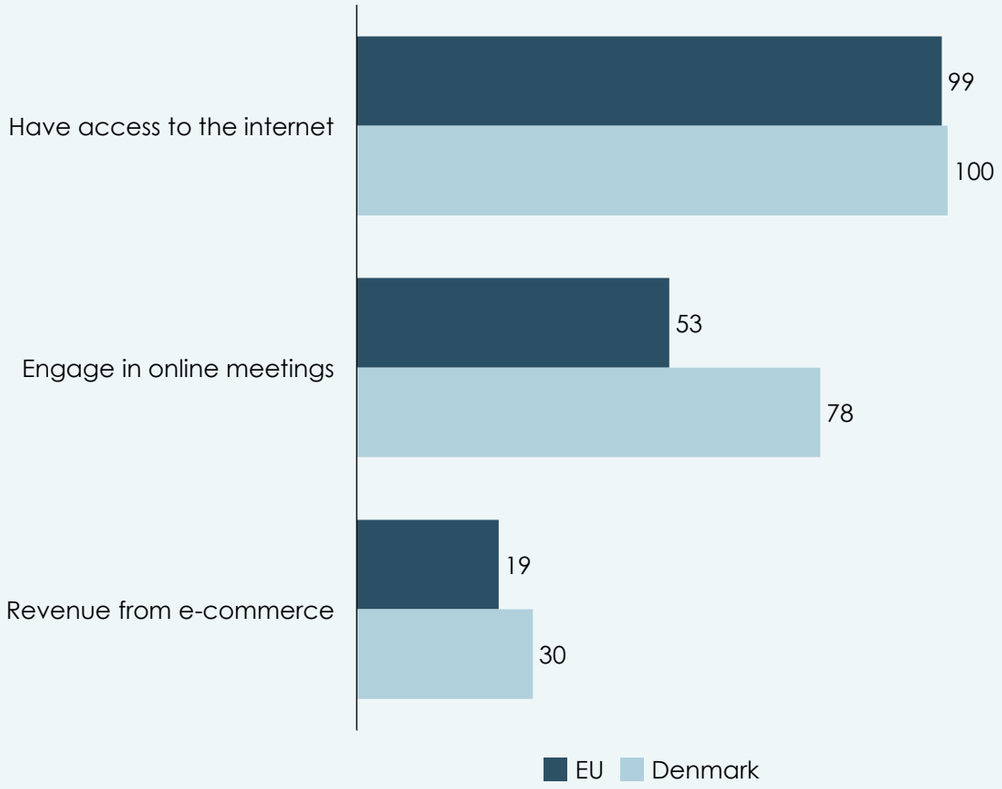
Second, TDC Net has a uniquely broad scope as Denmark's only operator with extensive activities across all major infrastructure layers, operating one of the most extensive backbone networks as well as both the largest fixed and mobile networks in the country, see Table 1 and Figure 3 in Box 2. Its network includes 820,000 fibre homes passed, 1,231,000 coax homes passed, and approximately 4,400 mobile antennas. TDC Net has consistently recorded the highest investment levels among Danish operators, see Figure 4 in Box 2.[4]

1) EU-NATO Task Force (2023). The resilience of critical infrastructure: Final assessment report. Link. 2) European Commission (2024): The future of European competitiveness, Part B. Link.

Telecom networks support important services for end-users in Denmark

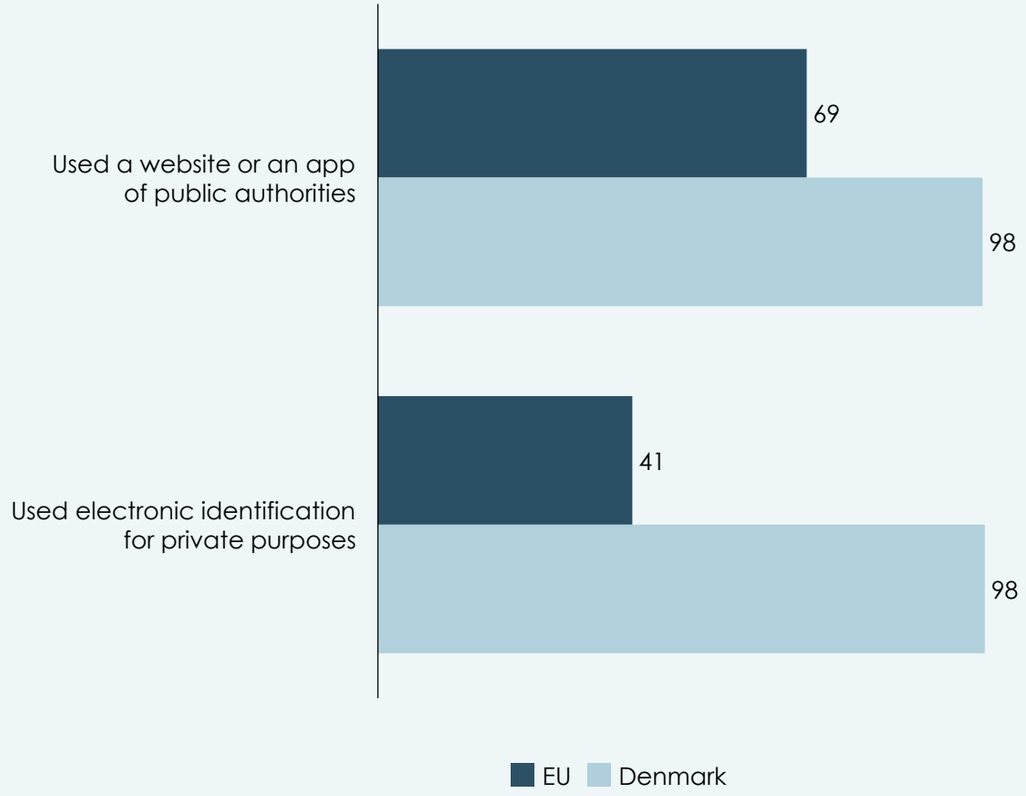
Box 1

Figure 1: European businesses rely extensively on the internet[1]
Per cent of businesses with at least 10 employees in 2024



Source: Copenhagen Economics analysis.

Figure 2: European governments rely on digital services to interact with citizens[2]
Per cent of citizens in 2023



Source: Copenhagen Economics analysis.

1) Eurostat (2026). Internet access by size class of enterprise. Link; Eurostat (2026). Meetings via the internet by size class of enterprise. Link; Eurostat (2026). Value of e-commerce sales by NACE Rev. 2 activity. Link. /
2) Eurostat (2026). E-government activities of individuals via websites. Link; Eurostat (2026). Use of electronic identification (eID). Link.

TDC Net plays a particularly important role in the Danish telecom sector

Box 2

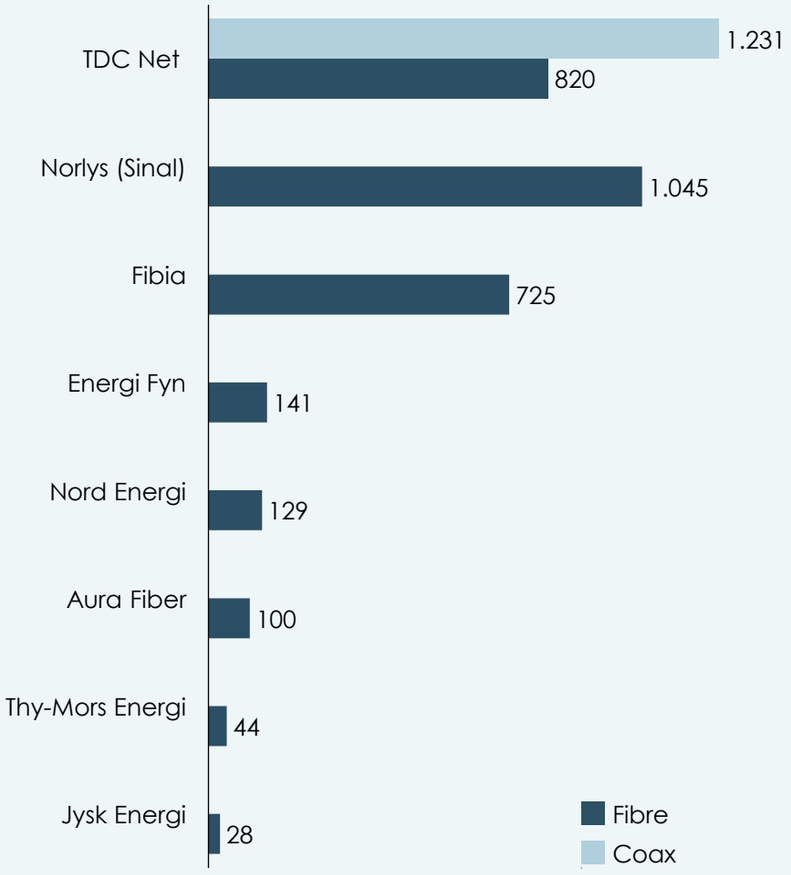
Table 1: Scope of TDC Net's backbone network[1]

Infra-structure	Number of connections in TDC Net's network
Internet Exchange Points	17
Core sites	12
Subsea cables with a landing point in Denmark (total subsea cables)	6 (ca. 80)
Regional aggregation networks	22
Edge sites	~1,000
Edge routers	~1,700

Source: Copenhagen Economics analysis.

Figure 3: High-capacity fixed line connections by largest operators[2]

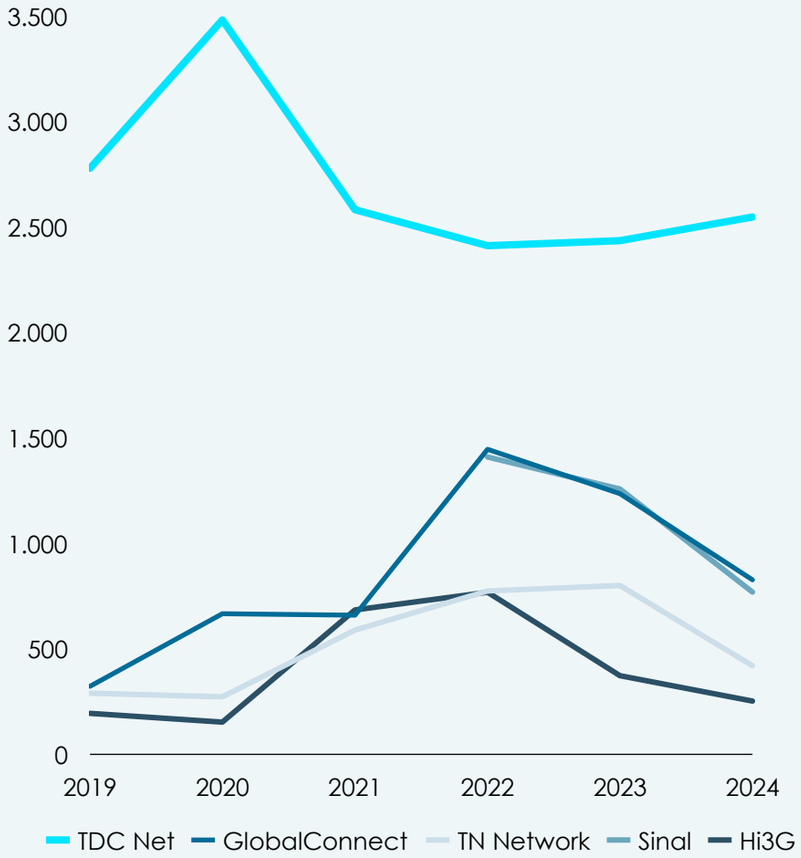
In thousands of households



Source: Copenhagen Economics analysis.

Figure 4: Investment by Danish telecom operators, 2019 – 2024[3]

In DKK million



Source: Copenhagen Economics analysis.

1) Copenhagen Economics, based on data provided by TDC Net. / 2) Copenhagen Economics, based on TDC Net (2026). Annual Report 2025, p. 10; Norlys (2026). Annual Report 2025, p. 20; Fibia (2026). Årsrapport for 2025, p. 8; Energi Fyn (2026). Årsrapport 2025, p. 5; Nord Energi (2026). Årsrapport 2025, p. 15; Aura Fiber (2024). AURA har nået en vigtig milepæl. Link; Green Power Denmark (2025). Elnet, fibernet og æbletræer lever også om 50 år. Link. / 3) Investments are defined as additions to property, plant, and equipment on the companies' respective balance sheets. We show Sinal data only for 2022-2024, when it was incorporated into Norlys Fibernet. In 2019-2021, Sinal was incorporated into Stofa Fiber. Copenhagen Economics, based on operators' annual reports.

The threat landscape has expanded (1/2)

1.2

Telecom networks are exposed to a broad and evolving set of threats

Telecom networks are exposed to a broad and evolving set of threats, including malicious cyber threats and physical attacks, system failures, third-party failures such as power outages, human error, and natural phenomena, such as storms or floods, see Table 2.

The diversity of potential incident types makes it difficult to anticipate where the next disruption will come from, and which assets will be impacted.

The complexity of the risk landscape is further amplified by developments in the global threat environment. Recent years have seen state-sponsored and criminal cyber campaigns targeting telecom and other critical infrastructures, extensive power blackouts, and even full-scale war.

Real-world examples illustrate that networks are increasingly being put to the test

Multiple events illustrate the types of threats to which telecom networks are exposed:

- In Ukraine, Russia's war has included large-scale attacks on communications infrastructure, such as the Viasat KA-SAT satellite network outage at the outset of the invasion,[1] and the 2023 cyberattack on mobile operator Kyivstar, which left millions of users without mobile and internet services.[2]
- In the Baltic Sea region, recent disruptions to undersea power and data cables have highlighted how physical attacks and suspected sabotage can directly threaten international telecommunications, including the Estlink 2 electricity interconnector,[3] and multiple fibre-optic cables such as C-Lion1,[4] and Elisa's Helsinki–Tallinn links.[5]
- The April 2025 Iberian Peninsula blackout illustrates how power failures can rapidly cascade into widespread connectivity outages. Electricity systems are under growing strain from electrification, variable renewables, and complex cross-border power flows.[6]
- Coordinated cyber attacks against telecommunications operators in Singapore,[7] as well as espionage-oriented intrusions into telecom providers in the United States.[8]

Table 2. Telecom networks are exposed to a broad and evolving set of threats

Threats		Description
Malicious actions	**Cyber threats**	• Incidents caused by malicious actors, such as a cyber-attack or physical attack
	Physical attacks	
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	**Power outage**	• Incidents triggered by a disruption of a third-party service such as a power outage (i.e. a supply-chain disruption)
	Other	
Human errors		• Incidents following a human error or mistake such as situations where a system worked correctly but was used incorrectly
Natural phenomena		• Incidents due to natural phenomena such as storms, floods, or earthquakes

Source: Copenhagen Economics based on NIS Cooperation Group (2018). Cybersecurity Incident Taxonomy, p. 9. Link.

1) Danish Ministry of Defence (2022). Russia behind destructive cyberattack against satellite equipment in the lead up to the invasion of Ukraine. Link. / 2) Reuters (2023). Ukraine's top mobile operator hit by biggest cyberattack of war. Link. / 3) Fingrid (2024). EstLink 2 electricity transmission link between Finland and Estonia has failed, investigation continues. Link. / 4) University of Washington (2025). Baltic Sea Undersea Cable Security. Link. / 5) BBC (2025). Finnish police seize ship suspected of sabotaging undersea cable. Link. / 6) Reuters (2025). Iberian blackout was first known caused by excessive voltage, report says. Link. / 7) Cyber Security Agency of Singapore (2026). Largest Multi-Agency Cyber Operation Mounted to Counter Threat Posed by Advanced Persistent Threat (APT) Actor UNC3886 to Singapore's Telecommunications Sector. Link. / 8) Skyhawk Security (2024). How did the Chinese manage to penetrate the entire communications infrastructure of the United States? How will the privacy of US citizens improve? Link.

The threat landscape has expanded (2/2)

1.2

The threat picture has changed in Denmark

Developments in recent years have resulted in a broader shift in the security outlook for Europe as well as Denmark. As Danish Prime Minister Mette Frederiksen has stated:[1]

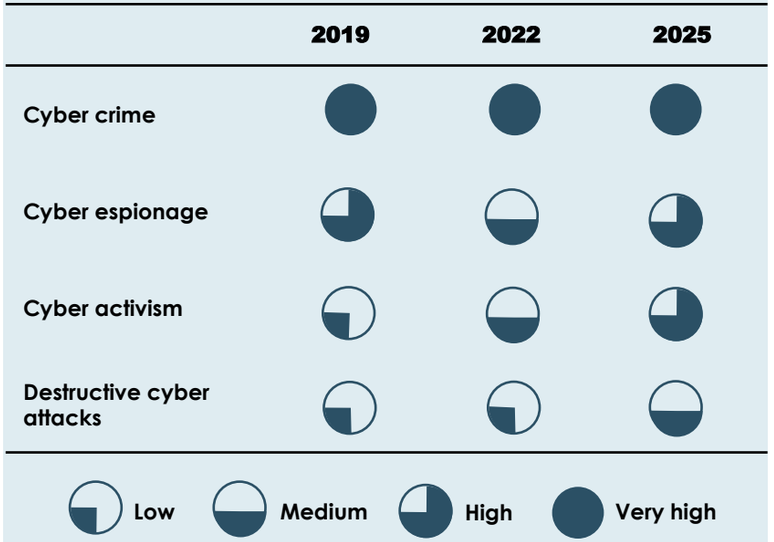
> *"We are not in a time of war, but we are also no longer in a time of peace."*

This underlines a need to build a more secure and resilient society across all essential functions, including the telecom sector.

The updated Danish threat assessment reflects this broader shift in the risk landscape. From 2022 to 2025, Denmark's Centre for Cyber Security raised the risk assessment for three out of four cyber threat types, with the fourth already at the highest possible level, see Box 3.

In parallel, the 2025 National Risk Picture concludes that Denmark faces its most serious risk and threat environment in decades and highlights cyber incidents as one of the most pressing cross-sectoral risks for essential societal functions, including communications infrastructure, see Box 4.

Box 3: Cyber threat to the Danish telecom sector



Source: Copenhagen Economics based on Center for Cybersikkerhed (2019, 2022, 2025). Cybertruslen mod telesektoren (see e.g., link).

Box 4: 2025 National Risk Picture

> *"Denmark is currently facing the most serious and complex risk and threat landscape since the Second World War. […]*
>
> *Security policy risks and threats, including the escalating hybrid threat, may have consequences for a wide range of vital societal functions and critical infrastructure, as well as for citizens' trust in the authorities. […]*
>
> *It is essential that we work together across sectors to address this complex and multifaceted risk and threat landscape."*

Note: Machine translated from Danish to English. Underlining made by Copenhagen Economics.
Source: The Danish Resilience Agency (2025). Nationalt Risikobillede 2025. Link.

1) "Vi er ikke i krigstid, men vi er heller ikke i fredstid", Prime Minister Mette Frederiksen stated at the 2025 annual Munich Security Conference. TV 2 (2025). Vi er ikke i krigstid, men vi er heller ikke i fredstid, siger Mette Frederiksen. Link.

Regulatory and societal expectations for resilience are rising

1.3

The current policy framework for the telecom sector covers multiple areas, including resilience

The Danish telecom market is currently affected by a broad policy framework[1] including various sector-specific legislations, some related to security and resilience specifically. Some of the most important regulations include:

- *SMP regulation:* sector-specific ex ante regulation designed to address competition bottlenecks in fixed broadband markets, e.g. fibre. This is EU-wide regulation implemented by national regulators (in Denmark, by Konkurrence- og Forbrugerstyrelsen) and approved by the European Commission.[2]
- The Broadband Fund is a state aid instrument that promotes rollout and coverage in commercially less attractive areas.[3]

See Table 3 in Box 5 for some of the most important regulations relating to resilience specifically. These include:

- *At the EU-level*, four core complementary regulatory frameworks exist. The NIS2 Directive classifies telecom operators as providers of essential services, and the CER Directive imposes on them obligations to ensure their resilience against various risks. The Cyber Resilience Act (CRA) requires operators' network equipment to meet distinct security-by-design and vulnerability-handling standards, while DORA can make operators subject to additional oversight.
- *At the national level*, the telecommunications security act (Telesikkerhedsloven) governs the security of supplier arrangements for critical network components, and the act on the centre for cybersecurity (CFCS) establishes CFCS's mandate to monitor, supervise and support critical infrastructure operators, including telecoms.

New resilience regulations will likely be implemented

At the EU level, new regulatory frameworks which include telecom operators in their scope are already in the works.

The revised Cybersecurity Act will seemingly impose additional requirements regarding the procurement of certain goods that are critical for telecom networks.[4]

The EU Action Plan on Cable Security sets out a coordinated response to the rising threat of sabotage and accidental damage to submarine and terrestrial cable infrastructure.[5]

The Digital Networks Act (DNA) will aim to harmonise existing telecom regulation within the Union with several distinct policies, and it also includes some initiatives relating to resilience.[6]

Further investment will be needed to increase the resilience of the telecom networks

Telecom operators will be required to continue and, in some cases, accelerate their investments in resilient telecom networks to respond to growing digital dependency, the expanding threat landscape, and increasing regulatory and societal expectations. As NATO notes, investments in critical infrastructure are needed to increase its resilience.[7]

> *"Since [critical infrastructure] enables critical government services and essential services to the population and economic actors, while also in some cases serving a security and defence purpose, governments must ensure that it is resilient to disruption.* ***This includes considering investment that may be necessary****." (our emphasis)*

Without such investment, the resilience of telecom services risks lagging behind society's reliance on them, increasing the potential for high-impact disruptions.

1) We use the term policy frameworks to refer to the entire set of policies, laws, and regulations that shape the telecom sector. / 2) The Danish Competition and Consumer Authority (2025). Vejledning om konkurrenceregulering af teleområdet. Link. / 3) The Danish Agency for Digital Government (2026). Bredbåndspuljen. Link. / 4) European Commission (2026). Proposal for a Regulation for the EU Cybersecurity Act 2026/0011. Link. / 5) European Commission (2025). EU Action Plan on Cable Security. Link. / 6) European Commission (2026). Proposal for a Regulation for the Digital Networks Act 2026/0013. Link. / 7) EU-NATO Task Force (2023). The resilience of critical infrastructure: Final assessment report. Link.

Telecom operators face multiple resilience regulations

Box 5

Table 3: Telecom operators face multiple security and resilience regulations (non-exhaustive list)

Regulatory framework		Objective
EU-wide regulation	The Network and Information Systems Directive (***NIS2***)[1]	Builds on the original EU-wide cybersecurity legislation (NIS) by responding to the growing threat landscape. Introduces stricter security requirements, streamlines reporting, and expands the scope to cover more sectors, including telecom operators, which 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 greater regulatory oversight.
	The Critical Entities Resilience Directive (***CER***)[2]	Aims to strengthen resilience frameworks by requiring providers of essential services to ensure their ability to withstand all types of disruptions, whether natural, intentional, or accidental. It builds on the previous Critical Infrastructure Directive of 2008 and expands its coverage to 11 sectors.
	The Cyber Resilience Act (***CRA***)[3]	Introduces EU-wide cybersecurity requirements for hardware and software products. It 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 that 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, which adds new obligations related to supply chain security.
	The Digital Operational Resilience Act (***DORA***)[4]	Under DORA, telecom operators are increasingly subject to scrutiny as critical third-party ICT providers to financial institutions. Designated entities are required to meet stringent requirements on ICT risk management, operational resilience testing, incident reporting, and third-party oversight.
Denmark-specific regulation[5]	The Telecom Security Act (***Telesikkerhedsloven***)[6]	Aims to safeguard Denmark's critical telecom infrastructure from national-security risks by enabling state oversight of, and intervention in, operators' supplier and vendor arrangements, including preventing arrangements that pose a threat to national security.
	The Act on the Centre for Cybersecurity (***CFCS-Loven***)[7]	Establishes Denmark's national cybersecurity authority with rights to monitor, detect and respond to cyber threats against critical infrastructure operators, including telecom providers.

1) European Commission (2022). Network and Information Systems Directive 2022/2555. Link. / 2) European Commission (2022). Critical Entities Resilience Directive 2022/2557. Link. / 3) European Commission (2024). Cyber Resilience Act 2024/2847. Link. / 4) European Commission (2022). Digital Operational Resilience Act 2022/2554. Link. / 5) Regulatory frameworks that not only concern the transposition of the depicted EU-wide regulations into Danish law, but also constitute separate national frameworks. / 6) The Danish Ministry of Resilience and Preparedness (2021). Telesikkerhedsloven. Link. / 7) The Danish Ministry of Defence (2019). CFCS-Loven. Link.

CHAPTER 2

TDC NET COULD FACE RESILIENCE INVESTMENTS OF UP TO DKK 4.7 BILLION BETWEEN 2026 AND 2030

Chapter 2 – Structure

2.1 Three scenarios for the level of resilience investments that TDC Net could face between 2026 and 2030	• Preparedness Level One: fit for current risk landscape: Commercial investments and compliance with current regulatory requirements. • Preparedness Level Two: fit for elevated risk landscape: Strengthen existing capabilities to meet increasing regulatory requirements and societal expectations. • Preparedness Level Three: fit for extensively elevated risk landscape – crisis ready: Prepare for unprecedented but plausible events that could become relevant under a changed risk assessment.
2.2 Each scenario is underpinned by a set of resilience investments	• An indicative and non-exhaustive list of investments. • Our analysis focuses on investment CAPEX. • Investment levels are highly uncertain.
2.3 The identified scenarios could result in investments of DKK 3.4 to 4.7 billion between 2026 and 2030	• Preparedness Level One: fit for current risk landscape: Approx. DKK 2,140-2,620 million investment • Preparedness Level Two: fit for elevated risk landscape: Approx. additional DKK 570-960 million investment • Preparedness Level Three: fit for extensively elevated risk landscape – crisis ready: Approx. additional DKK 720-1,170 million investment • Resilience investments in 2030 could correspond to around 40 per cent of TDC Net's total investment level in 2025

Three scenarios for the level of resilience investment that TDC Net could face between 2026 and 2030

2.1

The level of investment depends on societal needs
The level of investment required to strengthen resilience will depend on how the threat landscape continues to evolve, and how far Denmark chooses to raise its preparedness ambition.

We develop three scenarios for the level of security and resilience investments that TDC Net could face between 2026 and 2030, ranging from a preparedness level fit for current risk landscape to an elevated and an extensively elevated preparedness level, see Figure 5 and Box 6.

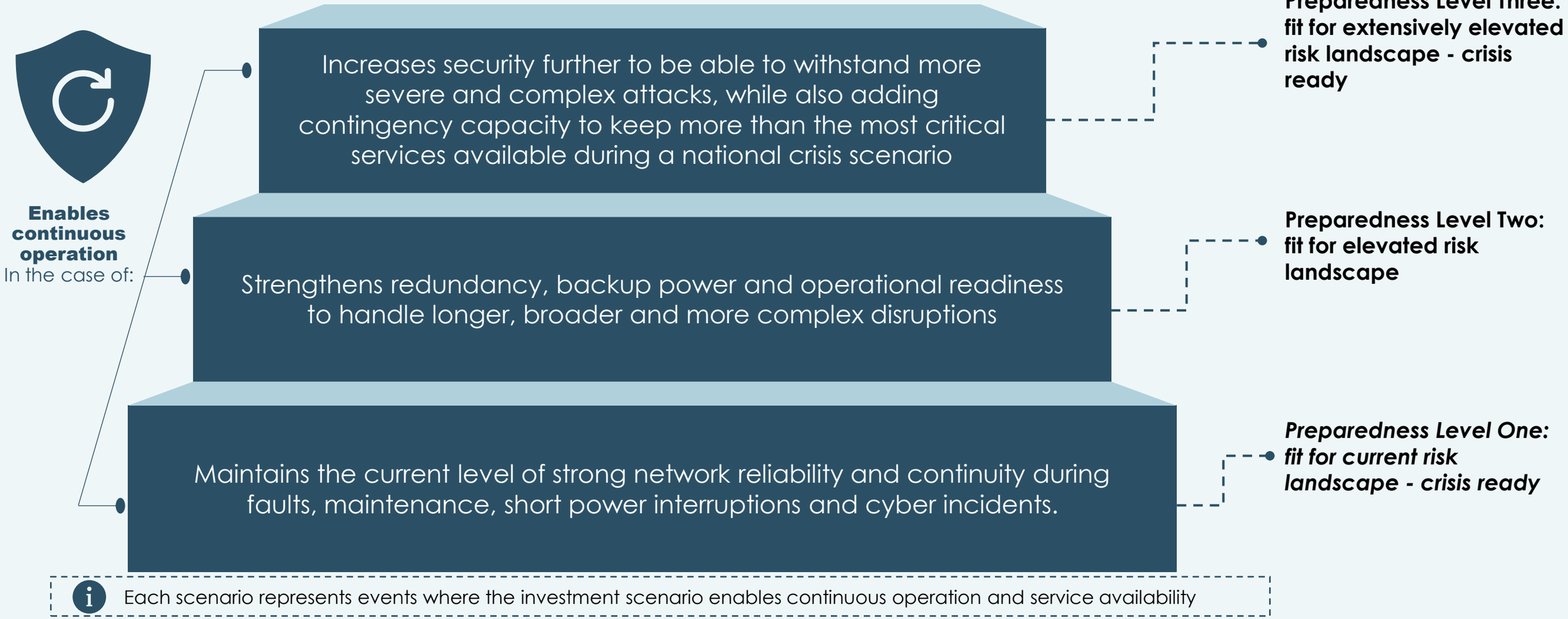
- **Preparedness Level One: fit for current risk landscape** reflects TDC Net's current resilience foundation, which is based on commercial interests combined with compliance with existing regulations. Investments focus on maintaining and renewing current capabilities through life-cycle management, technology upgrades, and continuous improvement to preserve service continuity under status quo disruption scenarios.
- **Preparedness Level Two: fit for elevated risk landscape** strengthens existing resilience capabilities in response to rising regulatory requirements and higher societal expectations. Investments go beyond the Preparedness Level One to improve the network's ability to withstand longer, broader, or more complex disruptions, while reinforcing continuity across physical, digital, and operational resilience.
- **Preparedness Level Three: fit for extensively elevated risk landscape-crisis ready** prepares for unprecedented, but plausible, events, such as conflict in Denmark, that could become relevant under an increased risk assessment. Investments are aimed at ensuring that critical services can continue even under extreme stress, through a higher level of redundancy, contingency capacity, and system-wide preparedness.

Figure 5. Three potential resilience scenarios for the future

Source: Copenhagen Economics.

Each scenario enables different degrees of continuous operation in the case of different events

Box 6



Note: The events are based on TDC Net's internal assessments.

Each scenario is underpinned by a set of resilience investments (1/2)

2.2

An indicative and non-exhaustive list of investments

To support the scenario assessment, we have identified a list of 43 potential investments spread across the different scenarios, see Boxes 9-11. These investments are based on discussions with TDC NET, insights into current resilience capabilities and investment needs, and examples of resilience measures observed in other countries. Identifying the relevant investments for each scenario is, however, inherently difficult, as future threats are uncertain, and the scale and timing of disruptions are hard to predict.

The resulting list should be seen as an indicative set of investment areas that illustrate what may be required under each scenario, rather than as a final or exhaustive investment plan.

The primary purpose of the investments would be to ensure the continued operation of secure telecoms infrastructure in Denmark, including during disruptive events. However, stronger resilience also makes the network a harder target, increasing the effort required to disrupt communications and thus reducing the attractiveness of deliberate attacks, i.e. potentially having a preventative effect.

Our analysis focuses on investment CAPEX[1]

Resilience-related investments are difficult to cleanly isolate as a distinct cost category, as they are embedded throughout network operations rather than appearing as a single, separable line item. They are reflected across network architecture, monitoring, maintenance, staffing, training, incident response and business continuity measures. Consequently, a significant share of resilience-related spending is integrated into day-to-day operations rather than dedicated investment programmes.

To estimate the cost of each investment, we focus on CAPEX, as this is the largest category of expenses related to resilience. Resilience measures may also increase OPEX, which would come on top of the CAPEX. For example, increased resilience would require a larger fleet of technicians that is ready to fix breakdowns fast.

Consequently, our approach is conservative in terms of evaluating the total potential financial implications of resilience.

The CAPEX investments have been grouped into four categories:

- Physical redundancy: Minimise service disruption through resilient network design.
- Power backup: Maintain operations during power outages.
- Operational readiness: Accelerate incident response and network recovery.
- Cyber security: Detect, prevent, and contain cyber threats.

Box 7: Investment scope in this analysis

We focus on investment within TDC Net's department called IT and Technical Services (ITTS). ITTS consists of the core systems that monitor, control and protect the network. Investments in these systems affect the resilience of the network as a whole, rather than only a specific local asset.

Other resilience-related investments may exist elsewhere in TDC Net's operations but are not included in this analysis. For example, in the department Delivery & Field Services (D&FS), CAPEX is primarily focused on last-mile fibre rollout, which expands coverage and capacity rather than directly improving resilience. However, some minor CAPEX investments relating to resilience could also be found in D&FS, e.g. locks to prevent tampering with street cabinets. Most of D&FS's resilience contribution is operational, through maintenance, repair capability and standby resources, and resilience efforts would therefore be reflected primarily in OPEX rather than CAPEX.

1) Capital expenditures (CAPEX) are funds companies spend to acquire, upgrade, or maintain long-term physical assets. In contrast, operating expenses (OPEX) are recurring costs necessary for the day-to-day functioning of a business.

Each scenario is underpinned by a set of resilience investments (2/2)

2.2

The investment levels are highly uncertain

The CAPEX estimates for each investment stem from TDC Net's internal assessment, see Box 8. The cost of individual investments is inherently uncertain.

Furthermore, as the investment scenarios are based on indicative, non-exhaustive lists of resilience investments, this introduces additional uncertainty in the estimated investment levels for each scenario. Some of the listed investments may ultimately prove unnecessary, while additional investments may be required to address threats that cannot currently be foreseen. As a result, the estimated CAPEX for each scenario should be regarded as an indicative estimate rather than a precise forecast.

In Boxes 9-11, we list the investments in each scenario and their corresponding cost estimate.

Box 8: Cost estimate methodology

The cost estimate for each investment stems from TDC Net's own calculations.[1] In total, 42 CAPEX investments are assessed across three resilience scenarios (Preparedness Level One: fit for current risk landscape, Preparedness Level Two: fit for elevated risk landscape, and Preparedness Level Three: fit for extensively elevated risk landscape – crisis ready).

For Preparedness Level One, the investments are taken from TDC NET's existing business plans for the coming years and rely on detailed project-level assessments of expected CAPEX.

The investments in Preparedness Level Two and Preparedness Level Three have not previously been developed in detail in TDC NET's business plans. Their CAPEX is therefore estimated using high-level bottom-up calculations. For example, the cost of adding a five-hour battery backup to all mobile sites is estimated by combining the average cost per battery and installation with the total number of sites.

1) With the exception of investment 31 (radar detection), which stems from Copenhagen Economics based on market intelligence. / 2) Capital expenditures (CAPEX) are funds companies spend to acquire, upgrade, or maintain long-term physical assets. In contrast, operating expenses (OPEX) are recurring costs necessary for the day-to-day functioning of a business

Preparedness Level One: fit for current risk landscape investments

Box 9

CAPEX grouping	Investments	High-level cost (DKKm)
Physical redundancy	Investment in network coverage, secure site access, geographically diverse core infrastructure, and transport redundancy.	1,080-1,320
Power backup	Investment in resilient power infrastructure, including battery backup, standby generation, mobile backup capacity, and dedicated operational support	150-180
Operational readiness	Investment in operational readiness through in-house expertise, vendor support, network operations capabilities, and crisis management	580-710
Cyber security	Investment in cyber security capabilities through in-house expertise, identity and access management, and continuous threat monitoring.	340-410
Total		**2,140-2,620**

Numbers may not add up to the total due to rounding.

Preparedness Level Two: fit for elevated risk landscape investments

Box 10

CAPEX grouping	Investments	High-level cost (DKKm)
Physical redundancy	Additional investment to further strengthen network resilience through enhanced redundancy, site hardening, and operational safeguards	160-190
Power backup	Additional investment in extended-duration power backup, expanded standby generation, and portable backup capabilities	300-420
Operational readiness	Additional investment in monitoring, predictive detection, and incident response capabilities	30-40
Cyber security	Additional investment in enhanced physical security controls, counter-drone capabilities, and third-party security requirements	90-320
Total		**570-960**

Numbers may not add up to the total due to rounding.

Preparedness Level Three: fit for extensively elevated risk landscape – crisis ready investments

Box 11

CAPEX grouping	Investments	High-level cost (DKKm)
Physical redundancy	Further investment in strategic resilience through independent communications capabilities, critical infrastructure hardening, and continuity of operation	610-1,020
Power backup	Further investment in additional backup capacity and energy storage to strengthen power resilience	100-130
Operational readiness	Further investment in enhanced continuity planning and emergency logistics	0
Cyber security	Further investment in strategic cyber resilience through independent network capabilities and future-proof cryptographic security.	10-20
Total		**720-1,170**

Numbers may not add up to the total due to rounding.

The identified scenarios could result in investments of DKK 3.4 to 4.7 billion between 2026 and 2030 (1/2)

2.2

Based on the scenarios and the underlying investments, we estimate that total CAPEX resilience investment could be up to between DKK 3.4-4.7 billion between 2026 and 2030, see Figure 6.

Preparedness Level One: fit for current risk landscape results in a DKK 2,140-2,620 million investment, approximately

- The key investments are in physical redundancy (up to DKK 1,320 million), which includes investments in geographically diverse core infrastructure and a transport network redundant to any single major failure.
- Operational readiness (up to DKK 710 million) and cyber security (up to DKK 410 million) investments also play a key role in ensuring a resilient network.

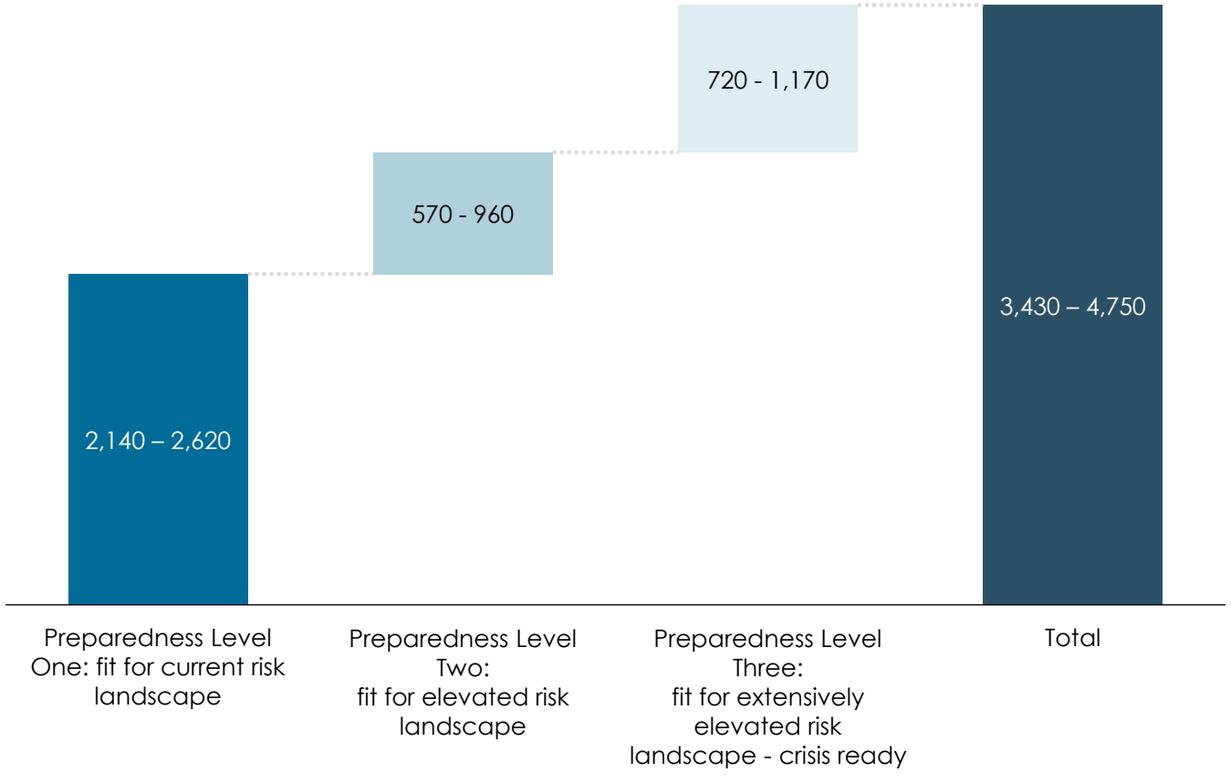
Preparedness Level Two: fit for elevated risk landscape results in an incremental DKK 570-960 million investment, approximately

- The key investments are in cybersecurity (up to DKK 320 million), such as greater third-party security requirements. Power backup plays a significant part too (up to DKK 420 million), with investments in extended-duration power backup and portable power generators.
- The total investment level would amount to DKK 2,710-3,580 million, including the cost of the Preparedness Level One.

Preparedness Level Three: fit for extensively elevated risk landscape – crisis ready results in an incremental DKK 720-1,170 million investment, approximately

- The key investments are in physical redundancy (up to DKK 1,020 million), such as having a parallel emergency network and increased infrastructure resilience.
- Power backup plays a part too (up to DKK 130 million), with further investments in portable generators.
- The total investment level would amount to DKK 3,430-4,750 million, including the costs of the Preparedness Level One and Two.

Figure 6. Investment levels in each scenario
Total CAPEX (DKK million), 2026–2030, approximate



Note: The ranges indicate the lower and upper bounds of the cost estimates.
Source: Copenhagen Economics based on cost estimates provided by TDC Net.

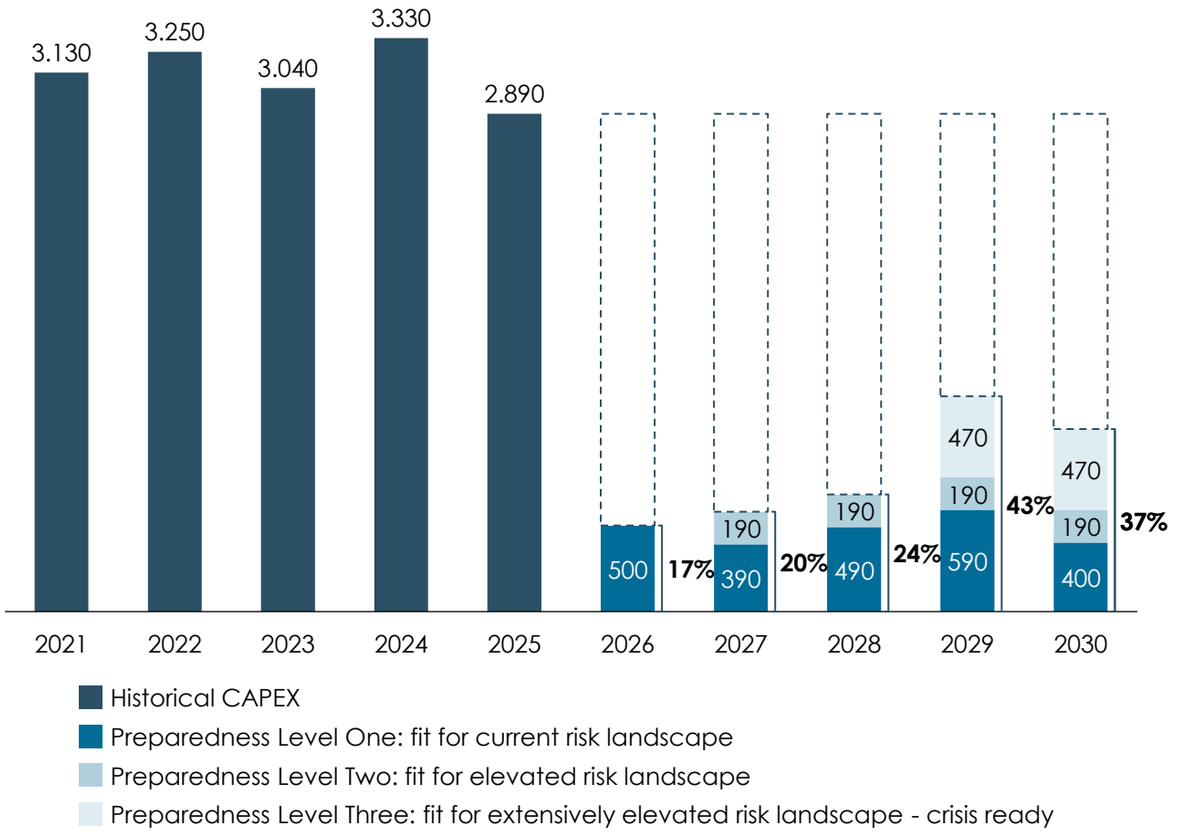
The identified scenarios could result in investments of DKK 3.4 to 4.7 billion between 2026 and 2030 (2/2)

2.2

Resilience investments in 2030 could correspond to around 40 per cent of TDC Net's total investment level in 2025

- The timing and sequencing of investments are subject to uncertainty. The optimal investment programme depends on the evolving risk picture, which is primarily assessed by the relevant authorities. Consequently, an ongoing dialogue between TDC Net and the authorities should inform decisions on which resilience investments to implement, and when. As the threat landscape changes over time, the required investments and their timing are, by definition, uncertain.
- TDC Net's Preparedness Level One already includes a significant commitment to invest in resilience and security, corresponding to DKK 400 million + p.a., with an exact timing of each investment.
- To show the potential investment level of the Preparedness Level Two and Preparedness Level Three resilience scenarios, we assume that Preparedness Level Two would begin to be implemented from the beginning of next year (2027), in line with the potential acute timing of growing regulatory requirements and societal expectations. Moreover, we illustratively assume that the risk assessment could increase by the end of 2028 in such a way that the Preparedness Level Three investments would have to be delivered quickly in a two-year period: 2029 and 2030.
- Under this time profile, we find that TDC Net's resilience-related investments in 2030 could correspond to around 40 per cent of its total investment level in 2025.
- Over the period 2021-2025, TDC NET has consistently invested around DKK 3 billion per year in its network. It is not possible to identify separately the share of these historical investments that is specifically related to resilience. However, the continuous modernisation and expansion of TDC NET's fixed and mobile infrastructure have contributed to increased resilience.

Figure 7. Future investments
DKK million, approximate



Note: Percentages indicate the total scenario-specific resilience investments as a share of total CAPEX investments in 2025. Cost in a given year is based on the midpoint estimates in the intervals
Source: Copenhagen Economics based on cost estimates provided by TDC Net.

CHAPTER 3

THE CURRENT POLICY FRAMEWORK WAS NOT DESIGNED TO SUPPORT RESILIENCE INVESTMENTS

Chapter 3 – Structure

3.1 Three market failures mean that the market will not deliver socially optimal resilience investments	• A public good: operators cannot capture the full social value of resilience. • Quality opacity: customers cannot easily observe resilience. • Coordination failures: no single actor has the full picture.
3.2 Investment obligations alone will not deliver desired outcomes	• Operators are unable to absorb the costs. • Asymmetric obligations will distort competition. • An overly prescriptive approach can encourage compliance rather than resilience.
3.3 The current policy framework should be revisited to ensure it reflects the policy priorities of today	• Current telecom regulation was designed primarily to address market power. • Regulation was not designed to address resilience-related market failures.
3.4 Any investment obligations should be accompanied by financing mechanisms	• Effective resilience is more likely to be achieved through shared incentives and collaboration than through obligations forced upon operators • Where strategic societal objectives go beyond commercial incentives, financing mechanisms should be put in place.
3.5 Three options for financing mechanisms	• Direct public funding / state aid • Compensation fund supported by a special levy on telecom services • Measures to strengthen operators' investment capacity

Three market failures mean that the market will not deliver socially optimal resilience investments (1/2)

3.1

Market failures mean that operators' investment in resilience would not align with what is socially optimal

In practice, operators may have a couple of commercial reasons to make investments in resilience, see Box 12. However, we have identified three reasons why the market may not work perfectly (i.e. "market failures"), meaning that operators will not deliver the socially optimal resilience investments, see Figure 8.

> ***Market failure -*** *a situation producing economically inefficient outcomes in which, under some conditions, public intervention may be indicated in order to improve social welfare.*[1]

On the following pages, we explain each of these three potential market failures in more detail.

Box 12: Commercial reasons to invest in resilience

- Some customers are willing to pay for superior security and resilience**.** This is visible when public authorities and other critical users make resilience and security explicit requirements in procurement, contracts, or operational standards. For example, government and emergency-response settings often require resilient communications arrangements to reduce the risk of service disruption during crises. Similarly, enterprise and institutional customers may require stronger service guarantees, compensation in the event of downtime, backup arrangements, or enhanced protection because communications failures can impose substantial operational costs on them.
- Telecom operators may face reputational risk if they do not adequately protect against breakdowns. High-profile outages often attract extensive media coverage, prompt public complaints, and can damage perceptions of an operator's reliability. This visibility means that disruptions can undermine trust in the operator's brand.

Figure 8. Three potential market failures

Market failures for resilience investments

A public good with a positive externality: operators cannot capture the full social value of resilience

Quality opacity: customers cannot easily observe resilience

Coordination failures: no single actor has the full picture

1) Ledyard, J.O. (2018). Market Failure. In: The New Palgrave Dictionary of Economics, 3rd edition, London: Palgrave Macmillan, pp. 8246-8251.

Three market failures mean that the market will not deliver socially optimal resilience investments (2/2)

3.1

A public good with positive externalities: operators cannot capture the full social value of resilience

Telecom resilience benefits far more parties than just the parties who pay for it. Stronger, more reliable networks help reduce outages and limit their impact on households, businesses, emergency services, and public authorities. This means that every improvement in resilience creates value across the whole economy, not just for individual users.

Because these wider benefits are shared broadly, telecom companies cannot fully recover the value of resilience investments through prices or individual contracts alone. In other words, the overall benefit to society is likely to be greater than the financial return to the companies investing. This creates a gap between private and social value, meaning that, left to the market alone, investment in resilience is likely to fall short of what would be best for society, see Box 13.

Quality opacity: customers cannot easily observe resilience

Resilience investments are difficult for customers to see, and the level of resilience can also be technical and difficult to understand. This means that end-users may not fully appreciate this dimension of quality when choosing their service provider. Instead, they focus on more visible and tangible features such as advertised speed, data allowances, and price.

This means that operators have limited ability to monetise resilience upgrades or above-and-beyond improvements, which weakens their incentive to invest in the first place. This is even though end-users might, if they could fully observe and understand resilience, seek a higher level of protection, see Box 14.

Coordination failures: no single actor has the full picture

A coordination failure exists when there is a two-sided information gap, when no single actor has the full picture. This is the case in relation to resilience investment, where the optimal investment decision depends on the risk picture and the investment costs. However, no single actor has the full picture, which creates a coordination problem with a risk of suboptimal decisions.

On one side, authorities usually have the best view of how important telecoms are for society as a whole, including links to emergency services, other critical infrastructures, and national security. They can, therefore, set high-level expectations for acceptable outage risks or recovery times.

On the other side, operators such as TDC Net know their own networks in detail and understand which specific technical measures are available, how effective they are in reducing risk, and which measures are the most cost-effective.

Because neither side has the full picture, the resulting level and composition of resilience investments may not be fully aligned with what would be best for society. Authorities may set requirements that are too low or too rigid, while operators naturally focus on solutions that make sense from a commercial and technical standpoint, given the information and incentives they face. This asymmetric information can mean that some cost-effective resilience measures are not taken up, or that resources are not always directed towards the investments that would deliver the greatest reduction in societal risk, see Box 15.

Market failure 1: A public good with positive externalities: operators cannot capture the full social value of resilience

Box 13

Public good: Telecom resilience has public-good features

In economic terms, a public good is one where:

- one person's use does not reduce what is available to others (non-rival), and
- where it is difficult to exclude people from enjoying the benefits (non-excludable).

Classic examples include street lighting or national defence: once they are provided, everyone in the covered area benefits, regardless of who paid. For such goods, the total benefit to society is often higher than the benefit any single buyer would be willing to pay for, so private markets on their own tend to provide too little of them.[1]

Defence is a classic example of a public good, where resilient telecom networks are a part of it. A more resilient network reduces the risk and impact of outages for all users connected to it, including households, firms, public authorities, and emergency services, even if only some of them pay directly for the underlying investments. One user's benefit from a stable network does not diminish another's (non-rival), and once resilience is built into the network, it is hard to confine its benefits to a subset of customers (non-excludable).

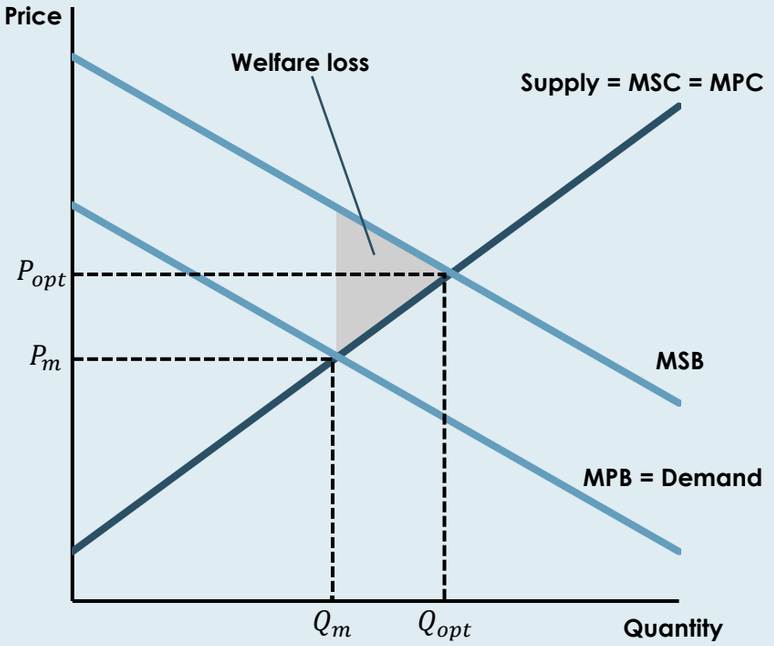
Externality: The social benefit of a resilience network exceeds the value for the individual consumers

A positive externality arises when the social benefit of an activity is greater than the private benefit captured by the firm making the decision.[2] In Figure 9, this is shown by the marginal social benefit (MSB) curve lying above the marginal private benefit (MPB) curve. Because the operator makes its investment decision based on the private benefit it can monetise, the market settles at Q_m. In this situation, the MPB equals marginal cost. This outcome is below the socially optimal level Q_{opt}, where MSB equals marginal cost. The grey shaded area illustrates the resulting welfare loss: society would benefit from more investment, but that extra value is not fully reflected in the operator's commercial return.

In the case of resilience investments, there is likely to be a positive externality, because resilience and security have strong public-good features. When an operator invests in resilience, the benefits go far beyond the customers who pay for the service. A more stable network helps businesses keep operating, enables public authorities and emergency services to function without interruption, and allows households to work, study, and communicate reliably. In other words, each reduction in outage risk for an individual user also reduces disruption risks for many others across the economy and society.

As a result, the operator does not capture the full social value of investments that reduce the probability or severity of outages. This can lead to resilience investment levels below the social optimum, even when additional investment would generate clear benefits for society as a whole.

Figure 9: Positive demand externality



Source: Copenhagen Economics

1) Sandmo, A. (2018). Public Goods. In: The New Palgrave Dictionary of Economics, 3rd edition, London: Palgrave Macmillan, pp. 10973-10984.
2) Laffont, J.J. (2018). Externalities. In: The New Palgrave Dictionary of Economics, 3rd edition, London: Palgrave Macmillan, pp. 4318-4321.

Quality opacity: customers cannot easily observe resilience

Box 14

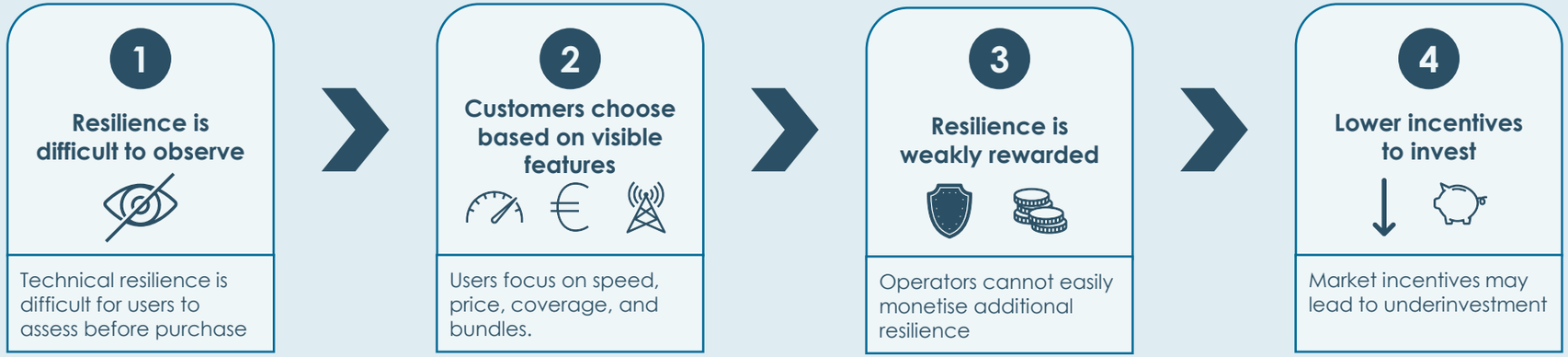
In economic theory, information problems arise when buyers cannot accurately observe or evaluate an important dimension of product quality at the time of purchase, even though sellers know more about it. When this happens, customers base their willingness to pay on what they can readily see and understand (such as price, brand, or headline performance measures), rather than on harder-to-observe attributes.[1]

Telecom resilience is a clear example of this. The level of resilience depends on technical design choices, redundancy, supply-chain robustness, and preparedness for rare but severe events, all of which are difficult for ordinary users to observe or assess. As a result, end-users may not fully appreciate this dimension of quality when choosing their provider, even if they care a great deal about avoiding outages.

Instead, users tend to focus on more visible features such as advertised speed, data allowances, handset bundles, coverage and price. Providers therefore compete mainly on these attributes, because they are the ones that most clearly influence customers' willingness to pay. Even where resilience is signalled through marketing claims or simple uptime statistics, these signals only imperfectly reflect the underlying level of protection.

Because resilience investments are difficult to observe and technically complex, operators have limited ability to monetise upgrades or 'above-and-beyond' improvements through higher prices or larger market shares. This means that resilience is systematically under-rewarded in the market, and operators have weaker incentives to invest in resilience than they would have if users could fully observe and understand the level of protection being offered.

Figure 10. Limited visibility of resilience can lead to underinvestment by telecom operators



Source: Copenhagen Economics

1) Postlewaite, A. (2018). Asymmetric Information. In: The New Palgrave Dictionary of Economics, 3rd edition, London: Palgrave Macmillan, pp. 510-513.

Market failure 3: Coordination failures: no single actor has the full picture

Box 15

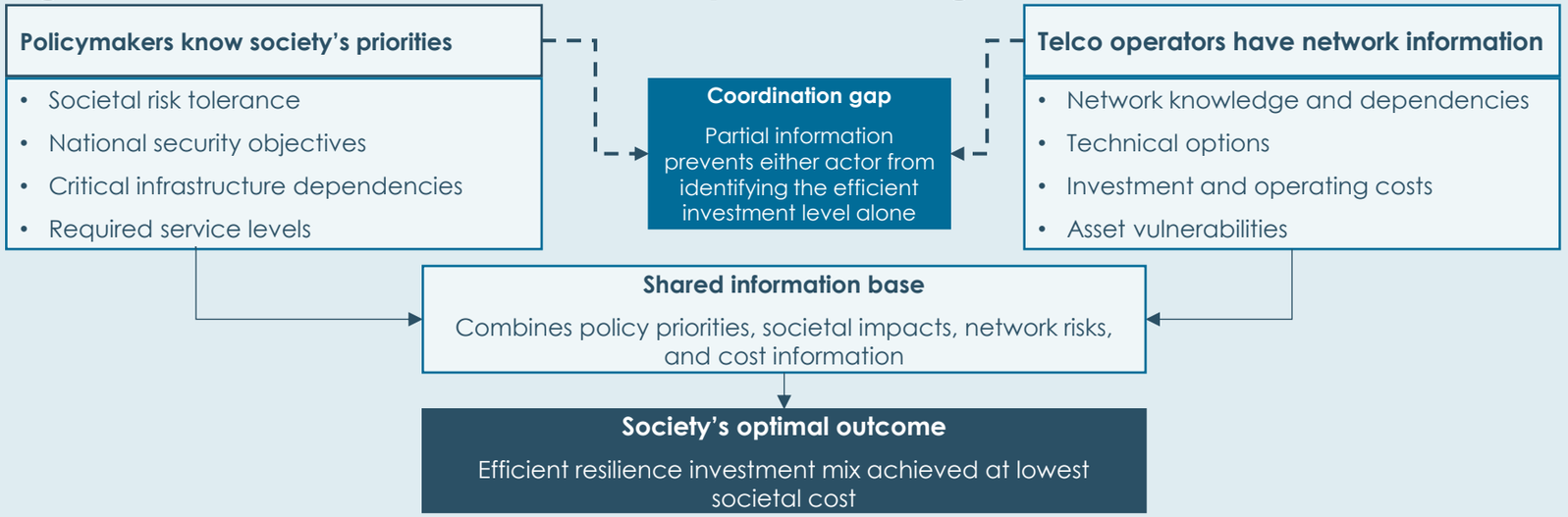
A coordination failure can exist when no single actor has all the information needed to make the best decision for society. On the one side, policymakers typically know more about overall societal risks, priorities, and acceptable levels of service. On the other side, firms know more about technologies, costs, and the concrete measures available. This situation is referred to as a two-sided information gap by economists.

When these pieces of information are separated, each side optimises based on its own partial view: policymakers set targets or rules without fully knowing the costs and effectiveness of different options, and firms respond based on commercial and technical considerations without fully internalising broader societal preferences. This lack of a single 'fully informed decision-maker' can lead to outcomes that are rational for each party individually, but not optimal from society's perspective.[1]

For resilience investments, there is likely to be a two-sided information gap. Policymakers and regulators usually have the best overview of how important telecoms are for the whole society, including links to emergency services, other critical infrastructures, and national security. They can therefore define high-level objectives, such as acceptable outage risks or recovery times. However, they often lack detailed insight into which specific technical measures are available in each network, how effective they are in reducing risk, and what they cost to implement. Operators like TDC Net, on the other hand, know their own assets, vulnerabilities, and cost structures very well, but do not necessarily see the full cross-sector consequences if parts of the network fail.

This split of information can mean that the resulting level and mix of resilience investments are not fully aligned with what would be best for society. Policymakers may set requirements that are either too low, because some risks are underestimated, or too rigid or costly, because they cannot easily distinguish between efficient and inefficient technical solutions. At the same time, operators will naturally focus on measures that make sense from a commercial and technical standpoint, given the signals they receive, even if other combinations of investments might deliver more societal risk reduction per euro spent.

Figure 11: Efficient resilience investment requires combining societal values with network risks and costs



Source: Copenhagen Economics

1) Ochs, J. (2018). Coordination Problems and Communication. In: The New Palgrave Dictionary of Economics, 3rd edition, London: Palgrave Macmillan, pp. 2286-2289.

Investment obligations alone will not deliver desired outcomes

3.2

Investment obligations are a regulatory tool whereby authorities could require telecom operators to undertake specific investments in defined assets or capabilities, for example, to strengthen network security or resilience.

In principle, such obligations could increase investment with the aim of closing gaps arising from market failures.

In practice, however, such an approach could lead to poor outcomes for three reasons.

Operators are not able to absorb the costs

If faced with investment obligations, telecom operators would most likely have to absorb most of the investment costs themselves. The reason is that it is difficult for operators to pass on the (full) cost of fixed-cost / sunk-cost investments to customers in both competitive markets and in markets subject to price regulation:

- *In competitive markets*, prices are driven by the marginal costs of providing the service, not by the total costs that firms incur. Resilience and security investments are largely fixed and do not change the marginal cost of serving an extra customer. This means that, even if operators face higher fixed costs due to new investment obligations, competitive pressure will keep prices close to marginal costs, and operators will have limited scope to increase prices to recover additional fixed cost investments.[1]
- *In markets subject to price regulation*, operators typically have limited pricing flexibility. The regulated prices are typically set using cost models that may allow only part of the new investment costs to be reflected in access charges, meaning that a material share of the costs would still need to be absorbed by the operator.

Danish operators may have limited scope to absorb additional resilience costs because the sector is already under financial pressure. A report by Deloitte for the Danish Agency for Digital Government ('*Investment perspectives in the Danish telecommunications industry*')[2] finds that Danish operators have weaker profitability than peers in other countries and that, under realistic forward-looking scenarios, the sector could operate close to a stressed position, leaving little headroom to cope with additional investment requirements, see Box 16.

Investment obligations may, therefore, crowd out other necessary investments in new technology and innovation. When operators are required to prioritise additional spending on resilience from already constrained cash flows, fewer resources remain for upgrading networks, rolling out new technologies, or developing innovative services.

Asymmetric obligations distort competition

Asymmetric investment obligations would distort fair competition between operators. If firms that compete against one another are subject to different resilience requirements, some will face higher costs than others for reasons unrelated to their efficiency or quality. This can create an unlevel playing field, weaken competitive pressure from disadvantaged operators, and ultimately risk worse outcomes for consumers in terms of prices, quality, or innovation.

An overly prescriptive approach can encourage compliance rather than resilience

An overly prescriptive design of investment obligations can blunt their effectiveness.[3] When regulation defines in detail which assets to build or which technologies to deploy, operators have strong incentives to focus on ticking compliance boxes rather than optimising for real-world resilience outcomes. This can create so-called 'moral hazard', with money spent on meeting formal requirements instead of addressing the most critical vulnerabilities, and can still result in underinvestment or investment in the wrong capabilities.

1) Vickrey, W. (2018). Marginal and Average Cost Pricing. In: The New Palgrave Dictionary of Economics, 3rd edition, Palgrave Macmillan, London, pp. 8206-8219. / 2) Deloitte (2026). Investment perspectives in the Danish telecommunications industry. Link. / 3) European Union Agency for Cybersecurity (2021). Guidelines on security measures under the EECC, p. 44. Link.

Danish operators are under financial pressure

Box 16

"International benchmarking shows that the Danish telecom operator sample delivers lower returns on assets and EBITDA margins than peers in Scandinavia, Europe, and North America."

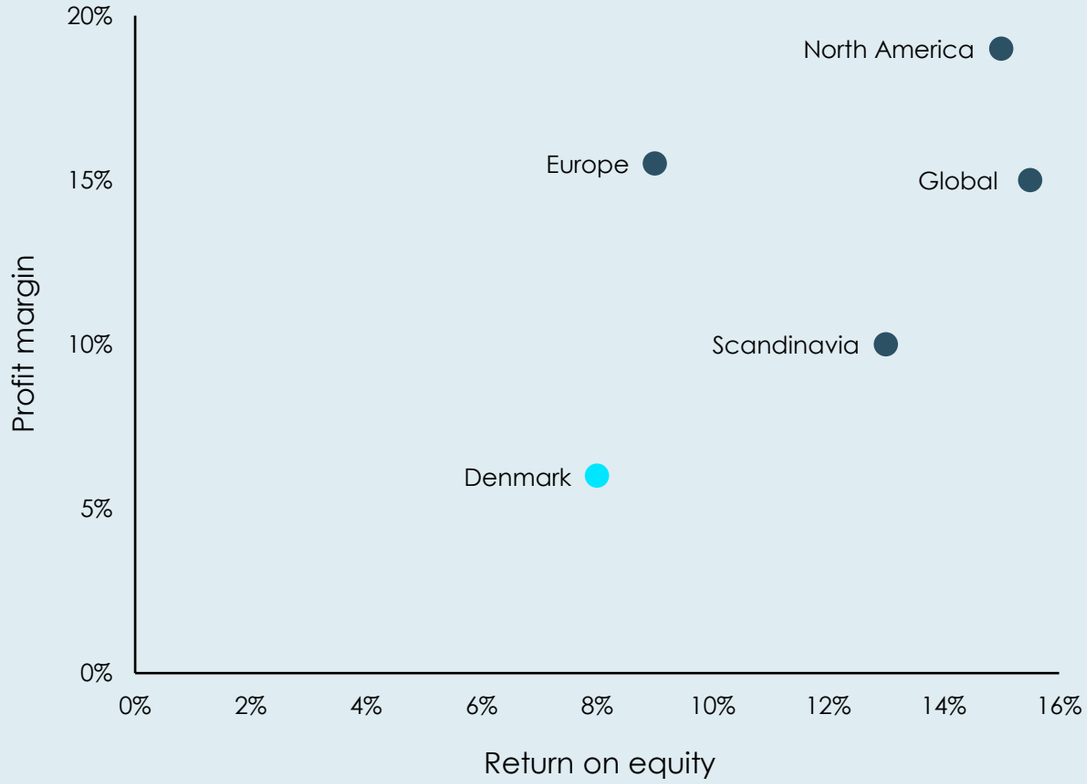
"Under the probability-weighted scenario in particular, the sector […] would operate close to a stressed position. In such a context, unexpected setbacks (such as weaker revenues, higher costs, or delays in realising returns on investment) could place renewed pressure on cash flows and financing capacity."

"In the absence of […] a turnaround, persistently low profits can constrain operators' ability to recover costs and attract external financing. This could adversely impact future network investments."

Source: Deloitte (2026). Investment perspectives in the Danish telecommunications industry. Link. Underlining by Copenhagen Economics

Denmark exhibits low profit margins and low return on equity

Figure 12. Operator sample financial ratio comparison



Source: Copenhagen Economics based on Deloitte (2026). Investment perspectives in the Danish telecommunications industry. Link.

The current policy framework should be revisited to ensure it reflects the policy priorities of today

3.3

Regulation is a tool for correcting market failures that arise when market outcomes do not deliver what policymakers want for society. Its purpose is to steer markets towards specific policy objectives.

The current telecom regulation was primarily designed to address market power

In European telecoms markets, the classic market failure has been market power: one or a few operators controlling key infrastructure could keep prices high or restrict access for rivals. In such a situation, competition alone may not deliver affordable services or efficient use of the network, because the dominant operator can exploit its position to earn excess profits and limit choice for end-users.

SMP (significant market power) regulation was therefore designed primarily to promote effective competition in fixed broadband markets and keep prices close to efficient cost levels. The main intervention has been to require the SMP operator to offer regulated wholesale access to its network at fair and reasonable prices, sometimes tied explicitly to costs, so that other providers can compete fairly at the retail level, see Box 17. This framework has been successful in driving competition and lowering prices.

The policy framework should reflect the policy priorities of today.

While SMP rules were designed for a world where the main concern was high prices and limited competition, recent years have seen a sharp increase in cyber threats, physical attacks, and climate-related hazards, alongside a much deeper reliance on digital connectivity across all sectors (see Chapter 1).

Accordingly, it is timely to revisit the policy framework, including SMP regulation and other potential policy tools, to ensure that it is aligned with today's policy priorities.

In Sections 3.4 and 3.5, we consider how the policy framework can be adapted to ensure that telecom operators can deliver the investments needed to meet society's growing resilience requirements.

Box 17: SMP regulation in Denmark

In Denmark, SMP regulation applies under the EU's telecom framework, which is implemented through Teleloven. The Danish telecom regulator, currently the DCCA, must identify relevant fixed wholesale access markets and decide whether one or multiple operators hold SMP in specific products and geographical markets.

In its draft decision for wholesale fixed broadband access, the Danish Business Agency (the former regulator) found an operator with SMP in 16 out of 18 geographical sub-markets. Fibia and Norlys were identified as SMP in two sub-markets, while all other operators, ranging from small regional operators to TDC Net, were SMP in at most one sub-market.[1]

When an operator is designated as having SMP, the DCCA must impose appropriate remedies. A typical remedy is to require the SMP operator to provide access to its network for a fair and reasonable (sometimes cost-based) price. In markets, where operators do not have SMP, they are free to charge commercial rates, since pricing is assumed to be constrained by competition.

1) The Danish Business Agency (2025). Udkast til analyse af konkurrenceforholdene på højkapacitetsmarkederne for bredbånd. Link.

Any investment obligations should be accompanied by financing mechanisms

3.4

Effective resilience is more likely to be achieved through shared incentives and collaboration

A collaborative approach between authorities and operators can help solve the coordination failure by creating structured processes to share data, scenarios, and technical assessments regularly. Instead of authorities guessing operators' costs and constraints, and operators second-guessing regulatory expectations, joint work on resilience can align views on what is needed, what it costs, and how quickly it can be delivered in practice.

This approach can help to operationalise operators' societal contract (in Danish: 'samfundskontrakt') by making explicit how telecom operators will contribute to society's expectations for resilient connectivity, and on what financial terms. By agreeing on shared objectives, principles for cost recovery, and priorities for implementation, authorities and operators can focus on delivering the necessary investments in a socially efficient way.

The importance of a collaborative approach is highlighted in the OECD report *Enhancing the resilience of communication networks:*

"Promoting collaboration and information sharing among network operators, emergency services and other stakeholders is a crucial strategy for enhancing network resilience."[1]

Where societal strategic objectives go beyond commercial incentives, financing mechanisms should be in place

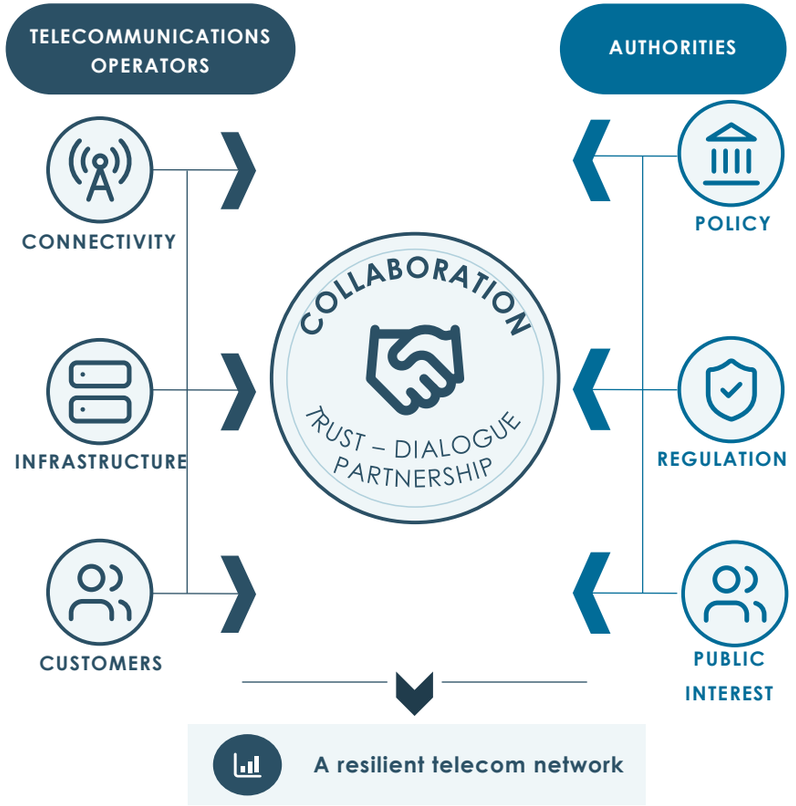
While a collaborative effort is important to identify the right level and mix of resilience investments, it does not in itself solve the problem that these investments create financial pressure on operators.

Collaborative planning can improve targeting and efficiency but still leaves open the question of who ultimately pays for the additional costs. Where public needs go beyond what commercial incentives alone would justify, dedicated financing mechanisms should, therefore, be considered to close the gap.

We find three potential financing mechanisms through which operators can cover the costs of resilience investments when they go beyond commercial incentives:

- *Measures to strengthen operators' investment capacity*
- *Compensation fund supported by a special levy on telecom services*
- *Direct public funding / state aid*

Figure 13. A collaborative approach to ensure resilient telecom networks



Source: Copenhagen Economics.

1) OECD (2025). Enhancing the resilience of communication networks, p. 28. Link.

Overview of financing options

Box 18

Financing model		Who pays?	Key strengths	Key limitations
Strengthen operators' investment capacity	**Less restrictive access price regulation in SMP areas** (for example: broader LRAIC, negotiation-based pricing, ex post checks, or partial deregulation.)	• Fibre customers in SMP areas	• Increases operators' capacity to finance resilience from own cash flows. • Expedient.	• SMP customers fund resilience investments through higher prices • asymmetric treatment of different operators' ability to finance investments. • Could be difficult to monitor effectiveness.
	Support economies of scale (for example, considering mergers or network-sharing agreements that allow operators to share fixed costs)	• Telecom users if consolidation harms competition	• Has the potential to improve efficiency.	• Could weaken competition at the expense of consumers. • Could be difficult to monitor effectiveness.
Sector/customer levy	**A compensation fund** that reimburses operators for (part of) the agreed resilience investments	• Telecom users	• Aligns costs with users of the infrastructure. • Provides funding through a dedicated compensation fund.	• Politically sensitive to introduce a new tax. • Administrative burden.
Direct state funding	**State aid resilience projects** (for example, grants or targeted programmes for critical-infrastructure upgrades)	• Taxpayers	• Strong fit when resilience has clear national security or societal value. • Transparent link to specific projects.	• Competes with other public spending. • State aid can be complex.

Three options for financing mechanisms (1/3)

3.5

Measures to strengthen operators' investment capacity

This option focuses on measures that strengthen operators' investment capacity, so they can finance resilience upgrades on their own balance sheets. Rather than creating new external funding streams, it aims to adjust the regulatory and competitive framework to give operators more room on their own balance sheets to invest in resilient networks. This can be achieved in at least two ways.

A first way of strengthening operators' investment capacity would be to loosen or remove access pricing regulation. Loosening could be done by, to a greater extent, accepting commercial agreements / voluntary commitments, shortening the price cap period, or applying an ex-post assessment of overall profitability. Removing would simply imply deregulation. The purpose of granting additional flexibility would be to allow operators to generate higher returns, at the expense of customers in those markets, to generate revenue to deliver on resilience investment requirements.

There are many examples across Europe of regulators employing looser approaches to access regulation. In some cases, there has been a complete deregulation, such as Norway, see Box 19. However, to our knowledge, loosening or removing regulation has never been done with the explicit objective of strengthening operators' finances to support investments (in resilience or in other areas).

While this approach to financing resilience investments could be relatively straightforward to implement, it would have implications for customers and could result in an asymmetric treatment of different operators' ability to finance investments, as follows.

First, in SMP areas prices would likely increase to the extent the access prices are passed through to retail prices. Thus, customers in those areas would compensate national resilience expenditures, spanning various network assets (including backhaul and mobile).

Second, if non-SMP operators were also required to invest in more resilient networks, these operators' ability to finance resilience investments would depend on the market context. In areas with parallel SMP and non-SMP operators, the non-SMP operators would expectedly follow an SMP operator's price increase by increasing their own prices, thus reaping the benefits of the SMP operator's greater pricing flexibility. In areas with only non-SMP operators, these operators' pricing is not constrained by regulation or competition and any changes to SMP regulation would have no impact. The non-SMP operators would not, however, receive additional funds to finance investments similarly to the SMP operators from areas where only a single SMP operator is present.

[continues on next page…]

Box 19: Deregulation for the SMP area in Norway

Norway's regulator, Nkom, fully deregulated for some operators in 2025.[1] Nkom found that the wholesale market for fibre tended towards effective competition because some operators had already committed to offering access on reasonable terms and because there was competitive pressure from mobile. Nkom also committed to continuing to monitor the market in case competition concerns emerged.

1) Nkom (2025). Varsel om vedtak om at grossistmarkedene for lokal og sentral tilgang til faste aksessnett (Marked 3a og 3b) ikke lenger kvalifiserer for sektorspesifikk regulering og opphevelse av forpliktelser. Link.

Three options for financing mechanisms (2/3)

3.5

A second way of strengthening operators' investment capacity would be to support economies of scale. Regulators and competition authorities could give increased weight to resilience and investment considerations when assessing scale-enhancing measures, such as mergers or network-sharing agreements. Within clear safeguards, this can allow operators to pool infrastructure, share fixed costs, or build larger integrated networks.

By improving economies of scale and scope, this option can materially increase operators' capacity to finance resilience investments from their own cash flows. It can also support faster roll-out of new technologies and more efficient use of existing infrastructure, to the benefit of service quality and coverage.

However, if not carefully designed and monitored, mergers or deep network-sharing arrangements can weaken competition, leading to higher prices or less innovation for end-users. There is therefore a need for robust case-by-case assessment and safeguards to ensure that gains in investment capacity do not come at the expense of competitive outcomes.

Both options (*more flexible access-pricing regulation and support economies of scale)* would have to be accompanied by strong accountability measures to ensure that additional investment capacity is actually used to strengthen resilience. Measures could include, e.g. clear investment commitments linked to predefined categories of eligible resilience projects and ring-fenced resilience capex within operators' investment plans (where appropriate). Greater transparency and reporting, e.g. through independent verification of resilience investments, would further support trust in the approach. Finally, adjustment mechanisms could help recalibrate the framework if threat levels, regulatory requirements, or technology developments change materially, so that investment efforts remain proportionate and well targeted over time.

Box 20: Support economies of scale

The new Draft Merger Guidelines acknowledge that mergers can be a way to support increased resilience investments. "*EU merger control supports the EU's broader policy objectives, including the competitiveness and resilience of the internal market*".[1]

In the UK, the Vodafone / Three merger was conditionally approved under binding network investment commitments. The merged entity claims it will invest GBP 11 billion in a faster and more resilient mobile network with improved capacity.[2]

Compensation fund supported by a special levy on telecom services

A sector or customer levy model would seek to finance resilience investments through a special charge on end-user telecom services (e.g. a 10% fee) which would be collected and paid into a dedicated compensation fund. This fund could then be used to reimburse operators for (part of) the additional costs of resilience investments, so that financing would flow from telecom users to the operators via a transparent mechanism.

A key strength of this model is that it aligns the cost of higher resilience with the users of the telecom infrastructure, who directly benefit from fewer and shorter outages. Because the levy is explicitly linked to a compensation fund and defined investment purposes, it can also make the financing more predictable and closely tied to the actual investment needs over time.

However, as with any new tax, a sector levy could be politically sensitive. Furthermore, implementing a new tax or fee and managing the fund would create an administrative burden (e.g. prioritising funds across different applications and managing complaints). The need to prioritise between different operators and investment types could also make it difficult to ensure that funding is allocated fairly.

[continues on next page…]

1) European Commission (2026). Draft Communication from the Commission: Guidelines on the Assessment of Mergers under Council Regulation (EC) No 139/2004 on the Control of Concentrations Between Undertakings. Link. / 2) VodafoneThree (2026). VodafoneThree completes world-first network upgrade by integrating core and radio sharing while unlocking access to its fastest 5G speeds. Link.

Three options for financing mechanisms (3/3)

3.5

Box 21: Direct state funding in Norway and the EU

Norway's Forsterket EKOM (FEKOM) programme funds enhanced resilience of privately operated mobile sites in vulnerable areas. In its 2026 budget, the Norwegian state has allocated NOK 210 million to FEKOM.[1]

The EU's Recovery and Resilience Facility (RRF) has given EUR 577 billion in loans and grants to member states. The RRF funds reforms and projects that aim to increase resilience and sustainability.[2]

Direct public funding / state aid

Direct state funding would mean that some or all resilience investments are financed directly from public budgets. In practice, the state can provide grants or targeted programmes for specific resilience projects, often linked to national security or critical infrastructure priorities. Under this model, taxpayers ultimately pay for the investments, reflecting that the benefits of resilient networks accrue widely across citizens, businesses, and the public sector.

A key strength of direct state funding is that it is well-suited where there is a clear national security or societal interest in raising resilience beyond what commercial incentives alone would justify. In addition, public budgets can be tied directly to specific, well-defined resilience projects, which makes the financing both transparent and closely aligned with the underlying investment needs. This can support clearer prioritisation, accountability for delivery, and a stronger connection between policy objectives and actual spending.

However, direct state funding must compete with other demands on the public budget, which can limit the political appetite, as well as create stop-start funding cycles. Furthermore, state aid can be associated with complexity, requiring careful design to avoid market distortions and to maintain strong efficiency incentives for operators.

Box 22: Sector levy in the Malaysian postal sector

Malaysia's Postal Service Fund (PSF) is envisioned as a collaborative, hybrid funding mechanism to support USO services and the development of the sector, with initiatives aimed at strengthening the sector's resilience, among other things.

All operators can submit applications for different initiatives, including safety and security enhancements.[3]

1) Norway's Ministry of Digitalisation and Public Governance (2026). Regjeringen bruker 210 millioner på å styrke mobilnettet – skal tåle strømbrudd i minst 72 timer. Link. / 2) European Commission (2025). The Recovery and Resilience Facility. Link. / 3) MCMC (2026). Public Consultation Paper on the Proposed Regulatory Framework for the Postal Service Fund Regulations. Link.

Copenhagen Economics

Hard facts. Clear stories.

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. Founded in 2000, we currently employ more than 80 staff operating from our offices in Brussels, Copenhagen, Helsinki, and Stockholm.

Learn more about our services.

www.copenhageneconomics.com