ISPA UK
THE VOICE OF THE UK INTERNET INDUSTRY

INCA
the independent networks cooperative association

Climate adaptation in the telecommunications sector

Fourth Adaptation Reporting Power (ARP4) report

December 2024

Table of Contents

Foreword

The need for fast and reliable digital infrastructure has never been greater. Nearly all aspects of our everyday lives – education, employment, communication, entertainment and more – are made possible by the continuous expansion and upgrade of telecommunications networks.

The Internet Services Providers' Association (ISPA) and the Independent Networks Cooperative Association (INCA) are delighted to submit this report under the fourth statutory Adaptation Reporting Power (ARP) to the Department for the Environment, Food and Rural Affairs (Defra).

This report marks the first time that ISPA and INCA have each formally reported to the ARP. Our aim for this report is to broaden the scope of evidence gathered, by including valuable insights from both large and smaller network operators in order to foster a more comprehensive understanding of the challenges and progress within the diverse landscape of the UK telecoms sector. We understand that the ARP reports are designed to highlight the risks and adaptation actions being taken by infrastructure sectors across the UK, and subsequently "raise awareness, build evidence, and make examples of good practice publicly available, encouraging innovation, investment and competition as demand for adaptation goods and services increases"[1].

ISPA and INCA are committed to ensuring a comprehensive understanding of the challenges and progress within the telecoms sector. Our involvement in this process aims to provide valuable insights into the specific vulnerabilities and adaptation measures relevant to our industry.

Internet Services Providers Association (ISPA)

ISPA is the trade association for providers of internet services in the UK, representing a diverse and dynamic membership that encompasses the full spectrum of the ISP sector, with approximately 200 members, ranging from SMEs to large multinational companies.

ISPA engages with policymakers, regulators, and other stakeholders to provide a unified voice for a diverse ecosystem, including operators that are building our future communications networks, and those that resell via fixed and wireless networks.

Our members provide internet access, infrastructure, hosting, and a wide range of other services to consumers and businesses.

Independent Networks Cooperative Association (INCA)

INCA is the leading UK trade association representing alternative organisations deploying independent digital infrastructure. Founded in 2010, INCA aims to foster a new approach to digital infrastructure, focusing on full fibre (FTTP) and high-quality wireless broadband whilst campaigning for the policy and regulatory support needed to maintain a healthy, competitive market.

INCA has over 200 members and represents most of the full fibre infrastructure builders commonly referred to as the Altnets. Members include network owners, operators, suppliers and managers as well as access networks, middle mile networks, network hubs and exchanges and organisations (including public sector) that are developing or promoting independent networks.

[1] Defra, *Climate Adaptation Reporting: Fourth round guidance* (2023)

Executive summary

This report, submitted under the fourth Adaptation Reporting Power (ARP4), provides an overview of physical, climate-related risks impacting the telecommunications (broadband) sector, current regulations influencing the resilience of networks, and the adaptive measures undertaken by the sector to prepare for the increasing frequency and severity of extreme conditions as a result of our changing climate.

Resilience is inherently built into telecoms networks, and national and international regulations and standards inform the short- and long-term management of our digital communications infrastructure. The sector is highly innovative, and is consistently working to improve upon and future-proof the networks, and ensure customers are protected and best served with necessary digital connectivity.

However, this report also acknowledges the barriers to adaptation – including interdependencies with other sectors, such as energy – and goes on to identify how the government can support the telecoms sector through information sharing and enabling cross-sector coordination.

As a critical national infrastructure sector, the telecoms sector recognises that climate change presents significant challenges and takes its responsibilities towards climate resilience very seriously, but also looks forward to opportunities for innovation and collaboration. This report serves as a call to action for continued partnership between the sector and the government to ensure a resilient and thriving digital future for the UK.

Introduction

The telecoms sector plays a vital role in the UK's economy and society, and its resilience to climate change is crucial. This report focuses on how climate-related risks could impact the sector, exploring the vulnerabilities of telecoms infrastructure and operations to extreme weather events, rising temperatures, and other climate-related disruptions.

Furthermore, this report aims to highlight the proactive steps the sector is taking to mitigate these risks and adapt to the changing climate, including strategies and technologies being employed to enhance resilience, from strengthening infrastructure to developing sustainable practices. The report aims to demonstrate the sector's commitment to ensuring continued service reliability and contributing to the UK's overall climate resilience.

This report marks the first time that ISPA and INCA are contributing to the Adaptation Reporting Power (ARP) process.

Organisational profile and scope of reporting

As the two main trade bodies representing the ISP sector, ISPA[2] and INCA[3] joined forces to prepare a sectoral overview response on behalf of the sector.

Methodology

In order to produce this report, our primary information gathering method was through a qualitative survey, followed by individual conversations with respondents to discuss their response and gather further insight. This was supplemented by conversations with other sectors to understand their perspective and approach, with government, as well as thorough background research and analysis into the state of climate change adaptation in the UK.

Although we initially looked at risk based on the approach in the most recent Independent Assessment of UK Climate Risk,[4] we decided to break these down into more specific risk factors, allowing us to draw out greater detail from reporting companies.[5]

Limitations

Although our memberships cover the breadth of the telecoms and internet sector, this report focuses on climate adaptation actions undertaken by the members which build and/or maintain communications networks, specifically on fixed and wireless access provision. It does not cover mobile or satellite networks and presents views at sector-wide, high level.

This project was also conducted on a voluntary basis, and respondents have been guaranteed anonymity within this report; therefore, we cannot comment on individual adaptation measures. As

[2] Internet Services Providers' Association

[3] Independent Networks Cooperative Association

[4] CCC, *Independent Assessment of UK Climate Risk* (2021)

[5] A full list of the risks shared with members can be found in the Annex.

this is the first report at this level, no comparison with previous reporting rounds can be made, although previous rounds have featured reports from techUK (ARP2, 2016)[6] and the EC-RRG (ARP3, 2021).[7]

Context for this report

Climate change in the UK

Climate change is already impacting the UK's infrastructure in a variety of ways[8]. Most notably – and topically – more frequent and intense rainfall has led to increased flooding, with Environment Agency data indicating that a record number of flood alerts and warnings were issued in Great Britain in the first four months of 2024[9], and the latter half of 2024 being dominated by further storms[10].

Other factors such as sea level rise, which saw "exceptionally high"[11] periods in 2023, are also accelerating – the most recent decade has been on average 1% wetter than 1981-2010 and 5% wetter than 1961-1990[12]. The UK is warming, with the top ten warmest years for the UK (since 1884) occurring since 2002 and the most recent decade was around 1 °C warmer than the pre-industrial period[13]. Ultimately, the UK climate[14] is predicted to become more unpredictable, and, as such, more severe, requiring the country's infrastructure and services to be prepared for any potential shock event.

Climate adaptation

For the purposes of this report, climate change adaptation is understood as the ability of a system to adjust to climate change (including climate variability and extremes), to minimise potential damage, to take advantage of opportunities, and to cope with the consequences[15].

Fourth statutory Adaptation Reporting Power (ARP4)

Under the Climate Change Act (2008) the Secretary of State for the Defra has the power to request reporting authorities[16] to produce reports on what they are doing to adapt to climate change, known as the Adaptation Reporting Power (ARP). This cycle (2024) is the fourth round of reporting.

[6] techUK, *The UK's core digital infrastructure: data centres* (2016)
[7] Defra, *Climate change adaptation reporting: third round reports* (2022)
[8] Climate Change Committee, *Independent Assessment of UK Climate Risk* (2021)
[9] Guardian, *Flood alerts at record level in Great Britain in first four months of 2024* (2024)
[10] BBC, *More rain forecast after Storm Bert hits UK* (2024)
[11] Kendon et. al., *State of the UK Climate 2023* (2024)
[12] As the atmosphere warms due to human induced climate change it can hold more moisture, at a rate of around 7% more moisture for every degree of warming (Met Office, 2024).
[13] Met Office, *UK Climate Projections: Headline Findings* (2022)
[14] In addition to the climate globally. IPCC, *AR6 Synthesis Report: Climate Change 2023* (2023)
[15] UKG, *Third National Adaptation Programme (NAP3)* (2024)
[16] Defined as "bodies with 'functions of a public nature' and 'statutory undertakers'" in: UKG, *Adaptation Reporting Power - FAQs* (2010)

Climate Change Risk Assessment (CCRA) and National Adaptation Plan (NAP)

Following the submission of this and other reports to the ARP4, these will feed into the next Climate Change Risk Assessment (CCRA4) and National Adaptation Plan (NAP4) and play a role in shaping the UK's future climate adaptation policy and overall strategy.

However, previous reporting cycles[17] identified a critical lack of information relating to the telecoms sector's climate vulnerability, which created barriers in the Government's ability to accurately assess preparedness for future climate change impacts. This underscored the need for more detailed reporting and analysis, such as this report.

Telecommunications: sector profile

The telecoms sector encompasses a wide range of services and technologies, creating complexity and variety in regulation, infrastructure, and service delivery. This section sets out the context in which the telecoms sector operates, giving a simplified overview of the types of operators present in the market, relevant regulation, and technology. We believe this is essential to understanding the latter sections of the report.

Types of operators present in the market

Although large and multifaceted, the telecoms (ISP) sector can largely be broken down into:

1. **Network operators**: companies that *build* and *maintain* the physical infrastructure that enables communication via the internet, predominantly through the installation and maintenance of full-fibre networks.[18]
2. **Service providers**: companies that provide the communication services via the physical infrastructure built by network operators. This can be to households, or to businesses.

Some companies are vertically integrated and are both operators and providers, whereas others may only focus on one or the other.[19] As we explain later on, the responsibility for climate adaptation largely lies with the network operator and many of these act as the wholesaler for a range of service providers and thus largely take on the responsibility for ensuring network resilience.

Other dynamics

All operators adhere to Ofcom resilience guidelines which provide for a high minimum threshold of physical and climate resilience. In addition there are a number of other factors at play which affect operator behaviour:

[17] Climate Change Committee, *Independent Assessment of UK Climate Risk* (2021); Defra, *Third National Adaptation Programme* (2023)

[18] ICO, *Key concepts and definitions* (2023); Ofcom, *Internet Service Providers (ISPs) and Network operators* (2023)

[19] This is a highly simplified explanation, solely for the purposes of this report. The sector can be broken down even further and greater nuances drawn from this, but we have opted for brevity in order to focus on how the sector *as a whole* is adapting to climate change.

- **Competitive Market:** The market is highly competitive and customers usually have a choice of network providers, thereby encouraging providers to build resilient networks.
- **Customer type:** Some providers specialise in serving businesses or critical national infrastructure (CNI) customers, and adopt additional resilience measures.
- **Maturity:** The market has seen an influx of newer providers – altnets – and is still in a growth and consolidation phase. Some of these newer providers adopt additional resilience measures[20] at an early stage while others will explore these options later on.
- **Locality**: Some ISPs operate on a national scale, with networks crossing the whole country, while others are highly localised, operating in urban or rural areas.[21]

Looking ahead, the next reporting period is likely to reveal a very different landscape, with new technologies, evolving business models, and ongoing consolidation[22] shaping the industry.

Technology upgrade: the communications network becoming more resilient

The telecoms sector is currently conducting one of the largest infrastructure projects in the UK to date. At the time of writing, 73.24%[23] of the UK has access to full-fibre[24] broadband, with the sector on track to hit the Government's own target of 85% gigabit-capable[25] broadband in 2025.[26] This is an expensive and complex process, including tens of billions of pounds of private investment, and involves upgrading consumers and businesses from slower copper connections[27] or no connections at all to full-fibre (and in some instances, wireless[28] or satellite[29]).

The rollout of full-fibre is being conducted in order to "future proof" the UK's communications networks – on the one hand, to accommodate increasing demands on the size and speed of data transfers, and on the other, to create a more physically resilient network. **Fibre is less susceptible to environmental fluctuations such as temperature or electromagnetic interference, and is inherently water-resistant.** This results in increased safety and reliability for customers and

[20] One way resilience and adaptation measures are established is through ISO certifications; this is explored later on.
[21] Perspectives from both national and regional ISPs have been included in this report. However, as noted above, we have not included detail around other technologies such as satellite, or mobile, focusing instead on fixed broadband / full fibre technology.
[22] For more information, we would recommend looking into Ofcom's Telecoms Access Review 2026.
[23] Thinkbroadband, *UK Superfast and Fibre Coverage* (2024)
[24] Full-fibre is considered the "next generation" of broadband and offers the fastest speeds and reliability compared to traditional (ultrafast or superfast) broadband.
[25] Please note that "full-fibre" is gigabit-capable, but not all gigabit broadband is full-fibre. For more information, please see articles including: USwitch, *What is gigabit internet?* (2024), USwitch, *What are the different types of broadband in the UK?* (2024).
[26] House of Commons Library, *Gigabit broadband in the UK: Government targets, policy, and funding* (2024)
[27] The copper retirement programme is evidence of the sector itself adapting to be more resilient in the future.
[28] Fixed wireless broadband, also called fixed wireless access (FWA), is a type of high-speed internet that uses radio signals rather than cables. For more information, please see: Ofcom, *Future of wireless broadband technologies* (2023)
[29] Satellite broadband is transmitted using a wireless connection via a satellite dish. For more information, please see: USwitch, *Satellite internet explained: is it any good?* (2024)

maintenance workers. Once the full-fibre rollout is largely completed, the traditional copper network will be retired.

Communications networks are built both underground and above ground ("overhead") with underground installation largely being placed in ducts and overhead installations using telegraph poles or wireless masts. Additionally, networks require a range of overground network components such as equipment and cabinets.

Network domains & infrastructure sharing

Network architectures differ between providers, but at a very simplified level, and can be broken down as follows:

- **Core**: seen as the "backbone", the core network is a high-capacity, long-distance network that forms the network's central structure;
- **Aggregation/Backhaul**: aggregates traffic and serves as an interface between the access and the core;
- **Access:** connects the core network to individual homes and businesses.

In most cases the level of physical redundancy increases for backhaul and core networks, but Ofcom guidance is clear that redundancy should be considered at the access level as well alongside requirements for power back up. A provider's responsibility for the network usually ends with Network Termination Equipment (NTE), modems or Optical Network Terminals (ONT, also known as a fibre box). Providers can also provide routers and other CPE.

There is a significant degree of shared infrastructure across network providers. Openreach, the largest network operator, has a regulatory obligation,[30] known as Physical Infrastructure Access (PIA), to provide access to its ducts and poles and operators can agree to share infrastructure under the Communications (Access to Infrastructure) Regulations 2016. The responsibility for resilience in these cases is shared but to a large degree falls on the network owner. Please see below for more information on Ofcom's Network and Service Resilience Guidance for Communications Providers, alongside the General Conditions of Entitlement.[31]

Regulatory overview

Our modern society is highly reliant upon communications technology, and as such the sector has for a long time been governed by a multi-layered legal and regulatory environment.

Ofcom: Resilience guidance

Ofcom recently updated its Network and Service Resilience Guidance for Communications Providers (the Guidance)[32]. In defining resilience in terms of "availability, performance, and functionality", the

[30] Ofcom, *Statement: Promoting investment and competition in fibre networks – Wholesale Fixed Telecoms Market Review 2021-26* (2020)
[31] Ofcom, *General Conditions of Entitlement* (2023)
[32] Ofcom, *Network and Service Resilience Guidance for Communications Providers* (2024)

Guidance lays out measures which telecoms providers are expected to take to ensure their networks are able to withstand physical risks, including climate change and severe weather[33].

The guidance also references the Cabinet Office's National Risk Register[34], the Government's Resilience Framework[35], and the framework for resilience outlined by the National Infrastructure Commission (NIC)[36].

Key measures:[37]

- When architecting a network, providers must ensure that networks are designed to avoid or reduce single points of failure, with specific regard for how many customers are connected to a site and how they could be impacted.
- Battery backup (minimum one hour, recommended four hours; must be sited in "active" cabinets) must be available as the first line of defence against power outages. More customers or premises means the site must be able to survive power losses for longer, potentially with permanent, refuelable back-up electricity generators (often diesel).
- Key infrastructure points should have automatic failover functionality built in, so that when equipment fails, network traffic is immediately diverted to another device or site that can maintain end user connectivity.
- Other measures providers are expected to implement to enhance physical resilience include equipment redundancy; physically separate and diverse connectivity; and fully automatic failover[38] between core sites (e.g. making use of separate resilient transmission links, dual parenting to separate core sites, resilient rings, and any other mechanisms that are appropriate).[39]
- Setting out the processes, tools, and training that should be considered to support the requirements on resilience.

In following this guidance, on a physical and technical basis, telecom networks are highly resilient to physical risk, in terms of both siting and contingency. From our conversations with members, all follow Ofcom's resilience guidelines.

National Infrastructure Assessment

The most recent National Infrastructure Assessment (2023),[40] overseen by the National Infrastructure Commission (NIC), gave an assessment of the United Kingdom's infrastructure needs

[33] In our conversations with members, it was acknowledged that Ofcom's resilience guidance helps many providers with designing networks which are resilient to climate change risk factors.

[34] HMG, *National Risk Register* (2023)

[35] HMG, *The UK Government Resilience Framework* (2022)

[36] NIC, *Anticipate, React, Recover - Resilient infrastructure systems* (2020)

[37] Also see: CCUK, Ofcom updated Network and Service Resilience guidance (2024)

[38] Automatic failover is a process that automatically switches to a redundant system when the primary system fails or becomes unavailable. It's a critical component of business continuity and disaster recovery, and is used to ensure that systems remain operational even when the primary system malfunctions.

[39] For example, a cabinet service area may be connected to other cabinets, with backhaul connections from each cabinet cluster to different datacentres with automated failover. This increases the resilience of a network if one part were to be disrupted.

[40] National Infrastructure Commission, *National Infrastructure Assessment* (2023)

to 2055 and beyond, including resilience. Some members participated in the reporting for this assessment.

TCFD reporting

The Task Force on Climate-Related Financial Disclosures (TCFD) is a government framework[41] that helps organisations disclose climate-related financial information. Under the framework, companies work to project how climate change could impact their networks in the future based on different scenarios, identifying potential physical, customer and organisational financial impacts.

As part of TCFD reporting, many companies in the sector are developing their approach to climate monitoring and management, such as conducting thorough climate scenario analysis of physical risks across sites; this is a rapidly evolving and innovative area, which is also leading to inter- and intra-sector partnerships and collaboration.

This information is published and publicly available.

Other regulation and guidance

- NPSA: Guidance on Protecting Buildings and Infrastructure[42]
- BDUK (DSIT): Environmental Resource Guide for Digital Infrastructure[43]
- Cabinet Office: Telecoms resilience[44]

Climate and the telecoms sector

Due to their importance for a modern, digital society, telecoms networks are designed to be resilient; however, increased frequency combined with increased severity of extreme weather events such as flooding and storms, plus longer-term shifts in weather patterns such as sea-level rise, precipitation and extreme heat can result in damage to physical and operational assets.

In general, across all our collected data and conversations with members, we noted that all are consistently looking to embed consideration of the effects of climate change into their core operational processes and longer-term business planning. Further, many also monitor changes in the business and regulatory landscape to understand where there may be opportunities resulting from the transition to net zero.

Below we give an overview of how certain identified risks affect telecoms networks, and some of the processes in place to protect against these.

[41] HMT, *Task Force on Climate-related Financial Disclosure (TCFD)-aligned disclosure application guidance* (2024)
[42] National Protective Security Agency (NPSA), *Building & Infrastructure* (2021)
[43] Building Digital UK, *Building Digital UK – environmental resource guide* (2023)
[44] Cabinet Office, *Telecoms resilience* (2019)

Key climate risks

Flooding: river/surface, coastal and groundwater

Climate projections for the UK indicate[45] there being a greater risk of heavy precipitation and prolonged events in the future, particularly during winter – meaning that when it does rain, it may be more intense, with a higher volume of rainfall happening within a given time period. This will increase the risk of flooding – both from river and surface water, as well as groundwater, as the soil becomes saturated and cannot absorb more,[46] which then sits on top of the land. In addition, even moderate increases in global temperatures, will have an effect on sea ice melting, which will lead to an increase in sea water, leading to potential coastal flooding.

For the telecoms sector, flooding is one of the most commonly identified risks. However, as identified by the CCRA3, "Ofcom requires all telecoms sites to be protected from flooding, and assets are generally located away from flood zones or at elevation."[47]

Companies have a high regard for flooding when siting both underground and overground infrastructure, and avoiding flood plains and areas at risk of flooding is often a key part of preliminary risk assessments. For instance, cabinets and poles are generally not sited on known flood plains, which serves to avoid the risk entirely. However, if the overground infrastructure is found to already exist on a flood plain, remedial work is carried out, such as protecting cabinets with added pumps or sealing tape, and standing cabinets on concrete plinths to raise their elevation (assessed regularly).[48]

While very extreme and localised flooding can impact underground units, the vast majority are already protected against water damage and have battery backup units installed in the event that power is interrupted.[49] Further, all respondents outlined automatic detection systems for network disruption, which logs issues and allows repairs to be conducted within hours (provided the site is accessible). It was noted, however, that flooding can interfere with providers' ability to travel around the country[50], and impact their ability to repair faults or even install new customers when sites are not accessible.

Some providers have flood alarms which are constantly externally managed (24/7). If there is extensive flooding of residential streets (particularly in cases when this is unusual), then underground equipment could hypothetically be at risk of water ingress. However, this poses a very

[45] Met Office, *The influence of climate change on severe weather*, 2024

[46] The fluctuation between intense flooding and drier conditions can increase the risk of subsidence, as noted below.

[47] Climate Change Committee, *Climate Change Risk Assessment (CCRA3) Evidence Report 2021: Telecoms and ICT Briefing* (2021), Pg. 6

[48] However, broadband is built to serve homes and businesses. If a development (i.e., a housing development) is sited on a flood plain, then this will come with a multitude of risks which will need to be mitigated.

[49] Interruption of power supply is cited as a key issue – this is explored further in the interdependencies section.

[50] Indicating an interdependency with the transport sector.

low risk, as the network is sealed against water ingress, and fibre cables will not be damaged if submerged in water.[51]

Additionally, for London-based ISPs, it was noted that the Thames Barrier poses a unique risk – if this were to collapse, then many networks (both underground and overhead) would be fundamentally compromised. However, it was also noted that this would constitute a catastrophic scenario, which would impact all infrastructure and public services in London. Therefore, it is recommended that, where possible, city-wide contingency plans are in plan to address this specifically, incorporating input from CNI operators.

High winds and storms

Most climate projections indicate that winter windstorms will increase slightly in number and intensity over the UK i.e., more winter storms, including disproportionately more severe storms.

High winds predominantly pose a risk to overground infrastructure, particularly poles and the attached equipment and cables. Strong winds can cause poles to fall, or cause trees to knock over poles or land on cables and equipment, detaching them from the infrastructure. However, newer poles are much less susceptible to being blown or knocked over,[52] and further, routine maintenance carried out by providers ensures that all infrastructure can withstand high winds and storms. Tree falls can indirectly lead to the damage of underground infrastructure, but this is considered less of a concern.

Further, there are health and safety considerations for engineers when working on overground infrastructure during high winds. Under the Health and Safety at Work Act 1974, "it shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees",[53] which necessitates the halting of working at height during strong wind. High winds can also interfere with providers' ability to travel around the country[54], impacting their ability to repair faults or even install new customers.

Unlike other factors such as projected temperature increases or higher sea levels, high winds (and their severity) are more difficult to predict in the long term. Members told us though that they do horizon-scan upcoming weather events through official sources such as the Environment Agency, the Met Office, SEPA etc to allow for potential interruption to be mitigated where possible.

High and low temperatures

Global temperatures have already increased by over 1°C since the industrial revolution. Whilst this increase may not seem significant, it has led to extreme heat events, such as heatwaves and record-breaking high temperatures, wildfires and melting sea ice. While extreme heat events do

[51] Copper and coax cables are more susceptible to damage from flooding; however, these are being phased out as part of the national infrastructure upgrade.

[52] The lifespan of a pole is usually around or over 20 years. As poles age, they can become more susceptible to decay, and therefore being knocked over by external factors. Regular maintenance is carried out by networks to ensure the strength and resilience of poles, minimising this risk.

[53] S.2, *Health and Safety at Work Act* (1974)

[54] Indicating an interdependency with the transport sector.

occur within natural climate variation due to changes in global weather patterns, the increase in the frequency, duration, and intensity of these events over recent decades is clearly linked to the observed warming of the planet.[55]

All of the respondents highlighted that temperature increases are a key concern, but one which is mitigated successfully. Cabinets are designed to work up to 45°C and cooling fans are used constantly to manage the temperature inside. Cabinets are also designed to work in temperatures as low as -40°C. When the UK temperature reached 40°C in July 2022, the record temperature in the UK[56], all respondents confirmed their networks continued to operate, demonstrating the resilience of the networks in the face of extreme heat.

Members also confirmed that temperature monitors are located within cabinets to notify operators when equipment is overheating, and, as identified within the flooding section above, members proactively horizon-scan upcoming weather events.

Subsidence: surface and underground infrastructure

Subsidence is a lowering or collapsing of the ground, usually occurring when the ground loses moisture and shrinks, often can be caused by prolonged dry spells. This can be exacerbated by more extreme climate fluctuations between intense flooding and hotter, more prolonged summers; additionally, factors such as soil type (clay being the highest risk) and vegetation can also have an impact.[57]

Although acknowledged as a factor of consideration and monitoring, members did not indicate that subsidence poses a significant risk to infrastructure. As noted above in the flooding section, infrastructure is generally never sited on known flood plains, and remedial work is often carried out to mitigate against this if needed. As noted by the CCRA3, while underground networks may be located in subsidence areas, "as it is more flexible than other types of buried infrastructure (e.g. gas pipelines) it is less vulnerable to minor earth movements."[58]

Other factors

Much as in the same way as high winds, lightning is impossible to predict in the long term. As the climate changes and storms are more frequent and of greater severity, factors such as lightning are expected to increase[59], although it is currently impossible to predict where and when.

This unpredictability is extremely difficult for companies to mitigate against beyond implementing current safety and resilience measures and proactively monitoring inclement weather which has potential to affect networks. However, it should also be noted that full fibre is less susceptible to damage from lightning strikes than copper because it is not an astro-magnetic conductor.

[55] IPCC, *Impacts of 1.5ºC global warming on natural and human systems* (2018)

[56] Met Office, *A milestone in UK climate history* (2022)

[57] BGS, *Swelling and shrinking soils* (2024)

[58] Climate Change Committee, *Climate Change Risk Assessment (CCRA3) Evidence Report 2021: Telecoms and ICT Briefing* (2021), Pg. 8

[59] With climate change, lightning frequency is estimated to increase by 12% for every 1°C warming. Romps et al., *Projected increase in lightning strikes in the United States due to global warming*, Science (2014)

Similarly, wildfires could occur more often in the case of extreme heat and prolonged dryness. The UK has not been significantly affected by large wildfires in the past, but this could change should the UK experience hotter summers with changes in precipitation. This is not currently regarded as a high risk to the UK telecoms sector.

Regional differences

Our research and engagement with ISPA and INCA members has demonstrated that there are regional differences in climate risk, but not necessarily in how the risk is mitigated. For example, networks operated in coastal areas must mitigate against potential coastal flooding, but how this is mitigated against is similar as if the network was being operated on in a floodplain.

Similarly, those coastal networks may experience stronger winds than centrally located networks, but the adaptation to that risk is the same in terms of potential damage to overground infrastructure from falling trees.

Regional variances in extreme heat have not been significant enough to note. As noted above, members have informed us that their networks can withstand extreme temperatures ranging from -40°C to 40°C which is currently inside the norm of what the UK experiences, even during extreme heat conditions; in the future, differences in how extreme heat affects networks in the north compared to the south may be witnessed.

Adaptation and resilience measures

Telecom operators must have an extremely high regard for resilience – not just because of Ofcom's Network and Service Resilience Guidance for Communications Providers, but also because of the investment landscape.[60] Companies must account for financial impact, customer experience and stakeholder perception in order to continue the rollout programme and generate a return, allowing future investment in resilience. An unreliable network which malfunctions during adverse weather may result in dissatisfied customers, meaning operators run the risk of losing customers to rival operators[61] if their networks do not perform as advertised.

Resilience standards

Overall, members take their resilience and adaptation measures very seriously. As an example of this, most have either already undertaken certification to ISO standards, or plan to, upon their businesses becoming more mature and they have the resources. This includes:

- ISO 9001 – Quality Management Systems

[60] In order for rollout to continue at pace, operators must provide a return for investors – this includes both private and state-subsidised. Therefore, it is in the interest of operators to build highly resilient networks from inception in order to maintain investor confidence and obtain further funding to continue rolling out full fibre.

[61] High levels of competition in the telecoms market means most customers often have the choice between multiple providers. For more information, please see: Ofcom, *Switching broadband provider* (2024)

- ISO 14001 – Environmental Management Systems
- ISO 22301 – Security and Resilience
- ISO 45001 – Occupational Health and Safety Management Systems

This has enabled operators to embed policies and procedures to aid their resilience efforts and business continuity planning, as well as embedding environmental management into their day-to-day operations. Importantly, the nature of ISO standards is an ongoing process with annual audits and certification, meaning that network builders who are certified to these standards are not "standing still", but it is a process of continual improvement and table-top exercises. Members who are certified do not consider these standards to be "tick-box" exercises, but rather have acknowledged the value they bring to their businesses to improve their resilience, security, and business continuity.

When a respondent indicated that they do not possess a particular ISO standard certification, they still have in-depth procedures in place to ensure networks do not go offline, or are reinstated as soon as possible in the case of an emergency. Reasons why some members are not yet ISO certified was primarily down to resourcing (factors such as cost, staff time, particularly affecting smaller and younger companies) but all indicated a desire or plan to embed the ISO standards into their internal policies and programmes in the future. It must be noted that of the ISPA and INCA members we consulted with, the vast majority had already achieved various ISO certifications.

Furthermore, there is a great deal of overlap between resilience[62], ISO standards, business continuity planning, and adaptation. Certain risk factors may not have been perceived within the context of climate change, yet there is a high level of preparedness nonetheless within the sector. In some cases, members have also used information and guidance provided by other network operators to help design their own resilience policies and procedures.

Flooding: river/surface, coastal and groundwater

Members are acutely aware of the risks posed by flooding and have taken proactive steps to minimise the risk. This includes, as noted above, designing networks to minimise flood disruption, using raised platforms or plinths for cabinets and using overground infrastructure (poles) in known flood plains. Further, some may deploy flood defences at higher risk sites including flood barriers, gates, and doors, and bulkheads.

In planning networks, operators risk-assess the designs and mitigate where appropriate. This is a constant and quickly evolving process, where operators are constantly learning and implementing new measures. This sometimes includes using climate projection data from reputable sources, and may contract the use of external experts to assist in the design phase. Further, collaboration with other bodies such as the Environment Agency (particularly in specific, higher-risk areas) is an example of how the sector can actively engage in long-term adaptation planning.

[62] Particularly Ofcom's Resilience guidance, as noted above.

High winds and storms

Members are proactively testing their networks to determine if they can be rerouted in areas which have proved vulnerable to storms in the past, but there is an acknowledgement that this may be limited in some areas, e.g. coastal areas where the wind is likely stronger.

Many have sought to become accredited to ISO 45001, embedding health and safety management into their daily operations, and therefore have a high regard for their engineers' health and wellbeing during extreme wind events; this would preclude engineers from climbing telegraph poles during a storm. Internal procedures dictate how long quickly a repair should be completed, e.g. within two working days (upon having access to the site).

High and low temperatures

All members are acutely aware of the issue of temperatures rising too much and affecting their networks and all mitigate this concern through cooling systems in the cabinets. Some members have proactively retro-fitted cabinets and installing cooling upgrades to ensure greater cooling power.

Members have also sought to become accredited to ISO 45001, embedding health and safety management into their daily operations, and therefore have a high regard for their engineers' health and wellbeing during extreme temperature events. Cabinets have temperature monitoring equipment built inside them so members can proactively monitor their equipment all day, every day. This would allow network operators to repair the equipment as soon as possible if it malfunctioned in the event of an extreme heat event.

Interdependencies

As one of the UK's CNI sectors, the telecoms sector is acutely aware of its position as a network upon which other sectors may rely – and at the same time, is highly dependent on other sectors as well.

Energy sector: electricity and gas

All of our reporting members cited a reliance upon the energy sector – especially electricity – as the most important interdependency, as virtually every component of a telecoms network, from the core network infrastructure to the customer's modem, requires electricity to function. Disruption to the energy supply can have immediate and cascading effects leading to service outages and potentially significant socio-economic repercussions.

Power back-up solutions are in place from vulnerable households to critical parts of the network, these ultimately have a limited lifespan. If the energy sector is down for a significant period of time, this is incredibly problematic for a network operator, which can impact other sectors and services.

The CCRA3[63] indicated that energy sites and networks were at significant risk from factors such as surface water flooding, and expected this to increase in the future. While full-fibre can be under water and still function accordingly, the main risk here is if the power networks fail, exacerbated by a lack of consistent communication from Distribution Network Operators (IDNOs) on where power is being restored.

There is an additional dependence in terms of gas and oil, as some operators rely on backup generators to keep their networks running in the case of a power outage.

Respondents expressed that the reliability of the energy sector needs to become a greater priority for government to ensure outages become less common.

Data Centres

Telecommunications companies rely heavily on data centres to support their core operations. Data centre facilities house servers, networking equipment, and storage systems, which are essential for managing network traffic, processing data, and hosting various applications and services.

Although data centres feature redundant power supplies and cooling systems to keep their services running, in the event of failure – or, notably, a power failure – this could significantly disrupt communications services.

Transport

Members expressed that transport is an interdependency for their operations, but described it as "secondary", in that the impact from flooding and high winds has the potential to cause issues with daily operations – roads could become impassable for engineers to access sites, potentially having an impact on the speed upon which a network outage could be rectified.

Water

Members expressed that the water industry could be considered as an interdependency in that there is a need for improvement in flood barriers and defences, and drainage systems to minimise disruption from flooding.

[63] Climate Change Committee, *Energy Briefing* (2021)

Barriers to adaptation in the telecoms sector

Climate data

Climate projection data is sporadic, inconsistent and hard to find. Members all acknowledge that factors such as flooding are expected to "increase", but there is a lack of specificity as to when, where and to what extent – climate projection data was noted as "inaccessible to non-climate scientists".

This hinders members' ability to have regard for climate change in their resilience and business continuity planning, particularly smaller companies which have less resource and capacity yet no less of a drive to improve upon their network resilience and future adaptation measures.

Inconsistencies in regulation and government messaging

Inconsistencies between government bodies and departments, and the very complex layering of the climate regime – particularly, between resilience, adaptation, sustainability, and net zero. Although telecoms resilience is largely overseen by DSIT,[64] as well as Ofcom; this request (ARP) came from Defra; further, DESNZ is responsible for net zero; the Cabinet Office oversees security; and local authorities also have both responsibility and duty to create their own plans, which can differ dramatically.

Additionally, constraints in legislation and data sharing between industry and government can hinder coordinated planning and response.

Cross-sectoral information sharing and collaboration

Inconsistent communication from DNOs about power restoration can hamper effective deployment of resources during outages.

Recommendations

Increasing and improving information from government

1. Work with climate and meteorological bodies to identify specifically how the UK's climate is projected to change – such as frequency and intensity of heatwaves, precipitation and flooding – and make this information widely available to infrastructure sectors.[65] The sector would benefit from this information when making long-term plans and increasing adaptive capacity.
2. Employ data sharing between industry and government to identify and prioritise support for vulnerable customers.

[64] Previously via the EC-RRG, although they did not report in this round.
[65] ISPA and INCA can help develop, share and get feedback on this information with our members.

Cross-sectoral information sharing and collaboration

3. Enable greater cross-sector collaboration by encouraging and facilitating data sharing and joint planning across interdependent sectors (e.g., telecoms, energy, data centres, transport).
4. Establish clear communication protocols for energy providers (particularly DNOs) to provide timely and accurate information about power outages and restoration efforts.

Working with local authorities

5. Work with local authorities, cities and infrastructure sectors to design and implement contingency plans that incorporate input from CNI operators and address risks like flooding, extreme heat, and storms.
   a. Additionally, ensure that local authorities are aware of the risks and detriments of building housing developments on floodplains.

Long-term, strategic action

6. Enable a strong investment landscape in order for the sector to continue the rapid pace of full-fibre rollout, and engage in groundbreaking innovation, such as digital twin technology.
   a. Enabling the investment landscape can include supply-side reform, and messaging from government regarding the importance of broadband rollout for the UK economy.
7. Develop learnings from other countries on adapting to climate risks. Other countries are already experiencing more intense and frequent climate disasters which the UK can learn from and develop adaptation plans based on issues which occur elsewhere.

Annex

ARP4: questionnaire for members – risk factors

- High temperatures
- Low temperatures
- High winds
- Lightning
- River/surface water flooding
- Groundwater flooding
- Coastal flooding
- Erosion
- Subsidence (risk to surface infrastructure)
- Subsidence (risk to underground infrastructure)

ISPAUK
THE VOICE OF THE UK INTERNET INDUSTRY

INCA
the independent networks cooperative association