GSMA

02



Futureproofing Connectivity

Weather-related risks and impacts on telecommunications networks

Copyright © 2026 GSMA

November 2026

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at **gsma.com**

Frontier is a strategic consultancy with an economics lens. We aim to deliver not just great analysis but the best possible outcomes for clients. To do that, we combine cutting-edge technical skills with a human way of working – bringing things like emotion, challenge, ambition, conviction, and a sense of fun. We help clients get things done well.

www.frontier-economics.com

Acknowledgements

This report has been developed by the GSMA with Frontier Economics.

The GSMA would like to thank members of the GSMA Climate Action Taskforce, Regulators, Network Equipment Manufacturers and Insurers whose expertise and valuable insights helped to shape this report series.

Copyright © 2026 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust notice

The information contained herein is in full compliance with the GSM Association's antitrust compliance policy.

Futureproofing Connectivity

This is the second report in a six-part series 'Futureproofing Connectivity: Climate Risk and Resilience in Telecommunications'. This collection of research identifies weather-related risks that telecommunications networks face, the associated financial impacts of these risks and what is needed to strengthen the resilience of networks in a changing climate.

By quantifying exposure to climate risk and showcasing best practices in network resilience, the research provides guidance for operators on climate-related planning, investments and reporting. The overarching goal of the series is to align the sector more closely and help prepare telecommunications networks for the impacts of a more volatile climate.













→ You can explore the other reports in the series here.

Report series structure

This research is split over a six-part series 'Futureproofing Connectivity: Climate Risk and Resilience in Telecommunications'

01
Executive summary and recommendations

Describes the research approach, key findings and provides practical recommendations for operators, policymakers, regulators, suppliers and investors to strengthen the resilience of telecommunications networks to the impacts of climate change.

02
Weather-related risks and impacts on telecommunications networks

Identifies acute and chronic weather-related risks and associated restoration costs that can affect telecommunications networks and maps these risks to different types of network infrastructure. This includes direct risks to mobile and fixed access networks, core networks, data centres, towers, backhaul, transport links and other supporting infrastructure. It also considers the sector's exposure to indirect risks and interdependencies, such as power supply and other critical systems.

03
Legal, regulatory and voluntary frameworks shaping network resilience

Assesses the resilience and adaptation obligations that telecommunications companies are expected to meet. These include telecoms-specific network resilience requirements, critical infrastructure obligations, corporate governance and risk management frameworks and climate-related reporting and disclosure frameworks.

04
Assessing weather- and climate-related risks

Reviews how operators currently assess risk. It covers the tools, methods, data sources, models and internal governance arrangements they use, together with the variables they need to understand the financial impact of physical climate risks and the cost of building resilience.

05
Prevention, response and recovery practices

Examines how operators respond to and manage weather-related risks in practice. This includes how resilience is embedded in network design, maintenance and renewal; the measures taken to reduce vulnerability and maintain service; how operators prepare for, respond to and recover from severe weather events; and how they manage the residual risks and financial impacts that cannot be fully prevented.

06
Annexes

Explains the methodology behind the modelling used to estimate infrastructure repair and replacement costs, and estimated telecommunications outages under current and future climate conditions. The inputs, sensitivities, assumptions and limitations are detailed, so that operators might use the approach in their own climate risk assessments.

Hazard, exposure and vulnerability

The reliability of telecommunications networks depends on the resilience of network assets to many types of threats, including severe weather. Weather hazards affect telecoms infrastructure directly, for example by damaging the network, or indirectly, by affecting network dependencies, such as power supply.

Severe weather risks are costly for telecoms operators, as they must repair damaged infrastructure and invest to strengthen resilience. Severe weather can also cause outages that not only cost operators, but also have impacts on users and across the economy.

This report introduces a framework for understanding weather-related risk based on hazard, exposure and vulnerability.[1] When hazards like severe weather affect exposed infrastructure, it creates vulnerabilities that can lead to loss of service or damage to infrastructure.

This framework is used to estimate the financial repair and replacement costs for cell sites associated with severe weather events under current and projected climate conditions. These costs are expected to rise over time as the frequency and severity of severe climate-related events increase.

Figure 1 **Framework for assessing weather-related risk**



1 This framework has been used by the IPCC since its Sixth Assessment Report (AR6). See: IPCC. (4 September 2020). The concept of risk in the IPCC Sixth Assessment Report: a summary of cross-working group discussions.



Acute and chronic severe weather hazards

When assessing severe weather hazards, operators should distinguish between acute weather hazards and chronic weather hazards.

Acute weather hazards are event-driven shocks. They are short-term atmospheric conditions and events, such as storms, cyclones, hurricanes, typhoons, intense rainfall, flash flooding, river flooding, coastal flooding, lightning, heatwaves, wildfire, snow, ice and severe cold.

These events can directly damage network assets or indirectly disrupt service through power outages, road closures, fuel shortages or supplier disruption.

Many are seasonal, but the timing, location and intensity of individual events remain uncertain. Operators therefore need to consider low-probability, high-impact events and select design standards appropriate to asset exposure, criticality and lifetime, such as 1-in-25, 1-in-50 or 1-in-100-year return periods.[2]

Chronic hazards are longer-term changes in average conditions. These include rising average temperatures, sea-level rise, changing precipitation patterns, higher sea temperatures, drought, water stress and changing wildfire conditions. They may not always trigger immediate outages, but they can change the baseline operating environment for network assets.

For example, sea-level rise amplifies coastal flooding; heat stresses batteries, electronics and cooling; drought increases wildfire risk and can constrain water-intensive cooling; and changing rainfall can increase the risk of flooding, landslides and ground movement.

More detail on climate forecasts can be found in Report 6, Annex 2.

2 A "1-in-100-year" event does not mean an event that occurs exactly once every 100 years. Rather, it means an event with a 1% chance of occurring in any given year. Similarly, 1-in-50 and 1-in-25-year events have a 2% and 4% chance of occurring in any given year, respectively.

Seasonal, cyclical and long-term weather hazards

The occurrence of weather hazards varies with seasonal, cyclical and long-term changes:

- Hazards such as tropical cyclones, winter storms, wildfires and heatwaves are seasonal and vary across regions.
- Medium-term climate cycles, such as El Niño and La Niña, affect rainfall, temperature, storm and drought patterns over months or years in particular regions.
- Over the longer term, climate change is expected to alter the risk of severe weather through higher average temperatures, sea-level rise and changes in precipitation patterns.

Operators therefore need to consider multiple time horizons. In the short term, they prepare for seasonal hazards, maintain assets and plan rapid restoration. Over one to 10 years, they incorporate weather-related risks into maintenance, investment and insurance decisions. Over the longer term, including to at least 2050 for long-lived assets, they need to incorporate these risks in site selection, design standards and technology choices.

Climate impacts of El Niño

El Niño is a regular, naturally occurring weather pattern that reaches a peak in a two- to seven-year cycle.[3] It is typically associated with hotter global temperatures, increased risk of drought and wildfire in parts of Australia, Indonesia and southern Africa, and heavier rain and flooding in parts of the Americas. 2026 is likely to see a very strong El Niño, raising risks of extreme weather into 2027 in some areas.[4]

Resilience, business continuity and adaptation

Operators have long managed weather hazards as part of general network resilience and business continuity. Climate adaptation adds another, forward-looking dimension, as operators need to assess whether existing arrangements will be sufficient in a more hostile environment where climate conditions are more extreme than today.

Resilience refers to the capability and capacity of a network to maintain and/or recover its ability to deliver mobile services to users in the face of disruptive scenarios. This involves the development of redundancy, robustness and recovery processes, and the ability to adapt infrastructure, people and processes so that essential services continue to function or can be restored quickly when disrupted.

Business continuity is the operational component of resilience: the plans, processes and capabilities used to prepare for, respond to and recover from an incident.

Adaptation is more forward-looking. It involves adjusting network assets, operating practices and investment plans where climate change is expected to alter the frequency, severity or geographic distribution of impacts on networks.

3 World Meteorological Organization (WMO). (2 June 2026). "WMO: Prepare for El Niño". Press release.
4 World Meteorological Organization (WMO). (3 June 2026). "El Niño set to become very strong, raising risks of extreme weather into 2027". Press release.

Climate projections and future risk scenarios

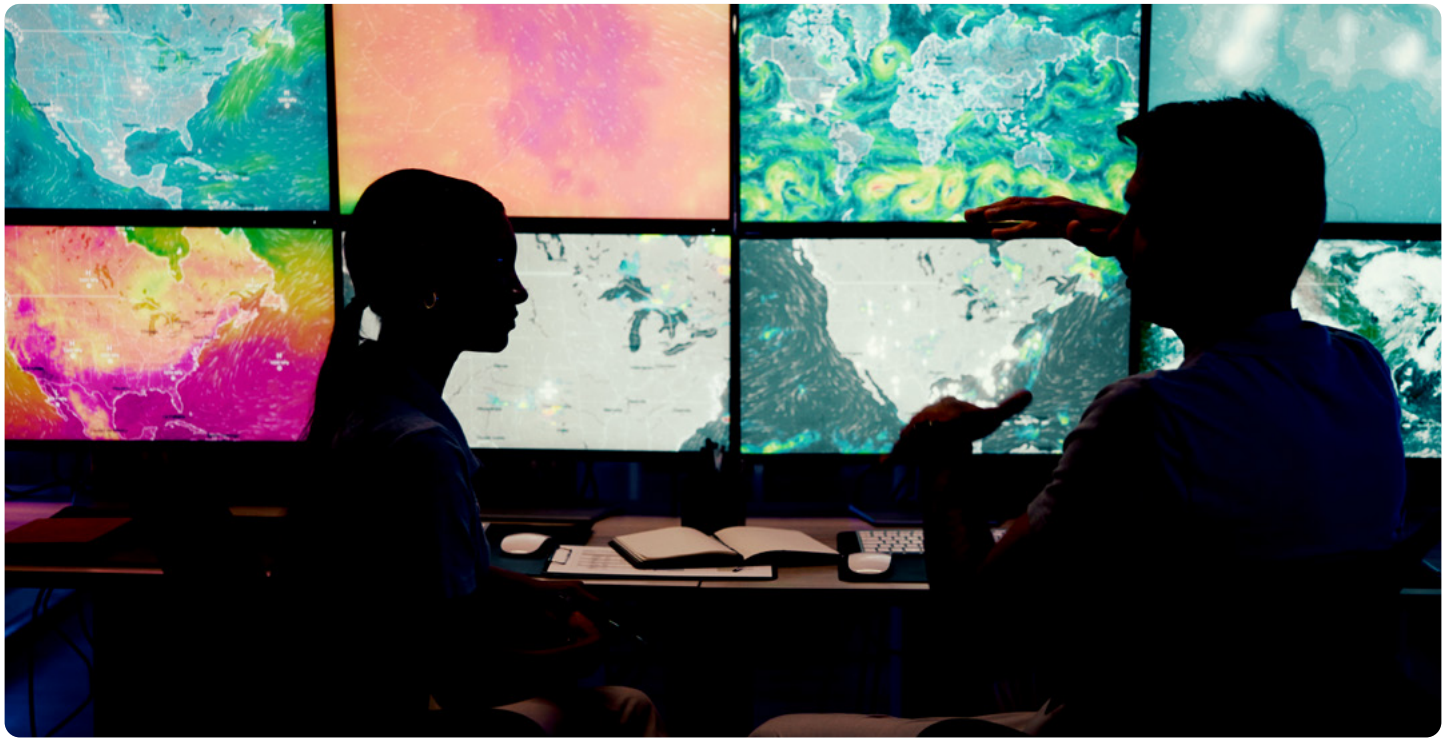
Climate forecasts and future risk assessment

The Intergovernmental Panel on Climate Change (IPCC)[5] periodically publishes major Assessment Reports (AR), which include forecasts of future weather patterns.[6] The most recent completed assessment cycle was the Sixth Assessment Report (AR6), with a Synthesis Report finalised in March 2023.[7] These reports bring together evidence from across three main areas: 1) the physical science basis of climate change; 2) impacts, adaptation and vulnerability; and 3) mitigation of climate change.

The weather projections contained in the reports are structured ways of testing how the climate system may respond under different future scenarios. These are labelled as Shared Socioeconomic Pathways (SSPs) and describe alternative futures for greenhouse gas (GHG) emissions, land use, air pollution, economic development and climate policy, which together affect weather patterns. They range from low-emissions pathways (SSP1–1.9), in which emissions fall rapidly, to high-emissions pathways, in which emissions remain high or continue to rise (SSP5–8.5).

These scenarios are not probabilistic forecasts. Instead, they provide a structured way to test how different emissions pathways could affect future temperature, sea-level rise and weather-related hazards. Typically, SSP2–4.5 is seen as a middle (more likely) scenario and SSP5–8.5 is a more extreme (upper limit) scenario. There is some discussion[8] that the "highest" plausible GHG scenario in the AR7 will be below the current SSP5–8.5 and the most pessimistic increase in temperature envisaged in AR7 assumes a maximum of 3.3°C temperature increase above pre-industrial levels, compared to a maximum of 4.6–4.9°C increase implied in AR6 and previous assessments.

The scenarios and limitations are described in Report 6, Annex 2.



5 The IPCC is the United Nations body for assessing the science related to climate change.
6 The IPCC is now in its Seventh Assessment Report cycle, or AR7, which is due to be published by late 2029.
7 The IPCC AR6 Synthesis report noted that, "Human activities, principally through emissions of greenhouse gases, have unequivocally caused global warming, with global surface temperature reaching 1.1°C above 1850-1900 in 2011-2020."
8 Hausfather, Z. (1 September 2026). "Explainer: The CMIP7 emissions scenarios – and how they explore future climate change". CarbonBrief.

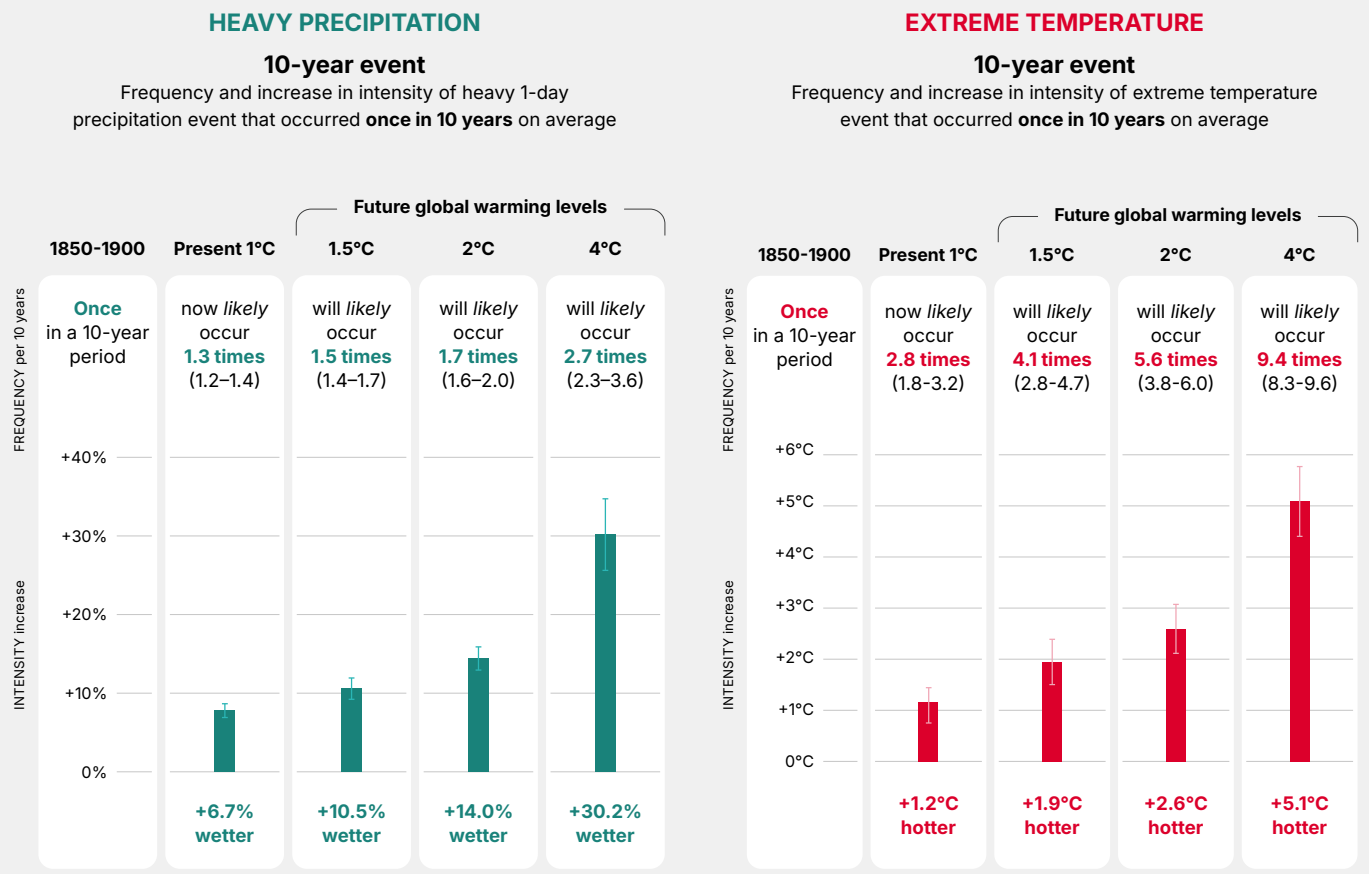
Climate change and changing weather hazards

The IPCC finds that climate change is already affecting weather and climate extremes in every region of the world: "hot extremes (including heatwaves) have become more frequent and more intense across most land regions since the 1950s, while cold extremes (including cold waves) have become less frequent and less severe".[9] At higher levels of warming, regional changes are expected to become more widespread and pronounced, including heavier precipitation and flooding in many regions, increased drought and increased fire weather in some regions and continuing relative sea-level rise along most coastlines.[10]

Figure 2 illustrates how heavy precipitation and extreme temperature events become more intense and more frequent as average temperatures increase.

- At 2°C of warming, a heat event that would once have occurred every 10 years is projected to occur about 5.6 times as often and be around 2.6°C hotter.
- A 10-year, heavy, one day precipitation event is projected to occur about 1.7 times as often and be around 14% more intense.

Figure 2 Frequency and intensity of heavy precipitation and extreme heat events



Source: IPCC AR6, Summary for Policymakers

9 IPCC. (2020). Summary for Policymakers. A.3, p. 8.
10 Ibid., B.2.

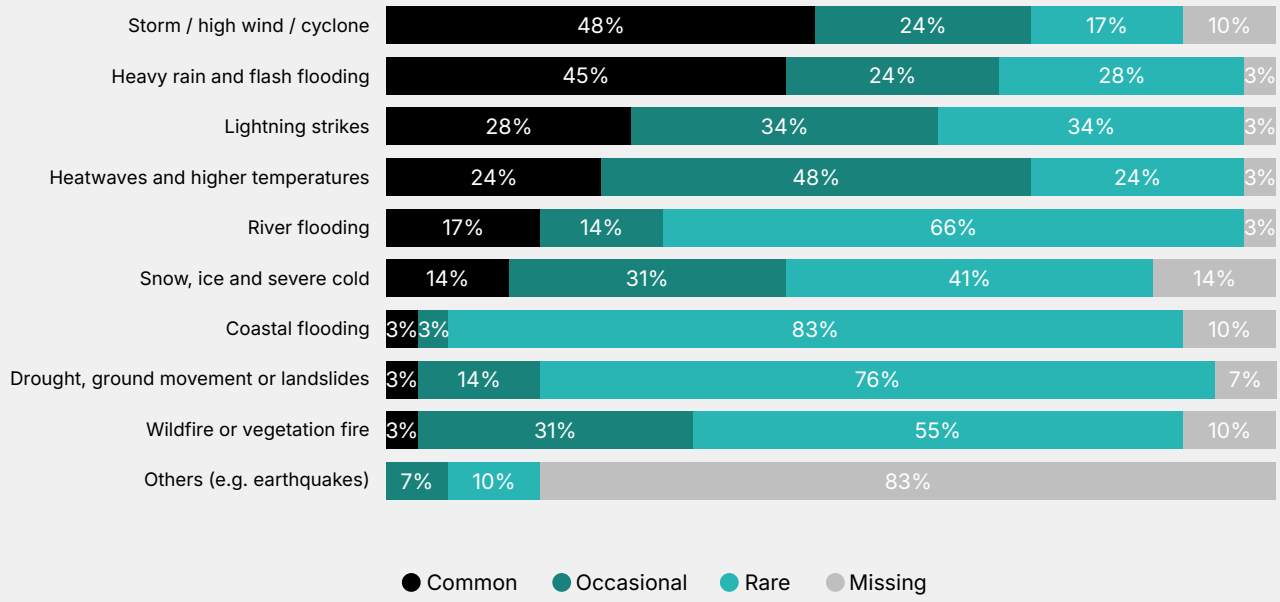
Risk by network layer and asset type

Telecommunications networks are exposed to weather hazards because they rely on geographically dispersed physical infrastructure.

Key weather hazards affecting telecommunications networks

Evidence from our survey, which is consistent with findings reported by operators in Carbon Disclosure Project (CDP) disclosures, shows that telecommunications networks are most exposed to flood, storms and heatwaves. Other hazards, such as wildfires, drought and coastal flooding, tend to be less frequent or more localised.

Figure 3 **Frequency of environmental hazards, as reported by operators**



Source: GSMA operator survey of 29 operators, consolidated responses dated 20 July 2026; Frontier Economics analysis.

Exposure by asset and deployment model

Exposure varies significantly by asset type and network layer. As Table 1 shows, fixed and mobile terrestrial access networks tend to have the greatest exposure to weather hazards because they include assets located across mixed terrain and, for mobile networks, often in elevated positions.

As networks expand to improve coverage or capacity, the aggregate physical exposure of the network increases, especially when new infrastructure is deployed in remote, coastal, mountainous, forested or otherwise hazard-prone areas.

Regional hazard profiles depend on the type of technology in use and how it is deployed. In many parts of the world, fixed access networks are still limited, which means connectivity depends primarily on mobile networks. Where fixed networks are deployed, exposure also depends on whether infrastructure is predominantly buried or aerial. As a result, two regions facing similar weather hazards may have different physical exposure profiles because their networks rely on different technologies or deployment models.

Table 1: Exposure of network assets to weather hazards

Hazard	Wireless networks	Fixed networks
Wind / storms	Towers, masts and rooftop sites are particularly exposed due to their elevated and dispersed locations. Strong winds can damage structures and equipment or misalign antennas.	Overhead lines and poles are exposed across streets, roads and vegetation corridors and can be damaged by wind, falling trees and debris.
Flooding	Ground-level equipment at mobile sites can be inundated. Core sites and data centres may also be affected by flooding, power disruption and restricted access.	Ducts, chambers and street cabinets are particularly exposed to flooding and water ingress, which can cause corrosion, short circuits and service degradation.
Snow / ice	Snow and ice can accumulate on exposed towers, antennas and dishes, potentially damaging equipment or causing signal loss.	Heavy snow and ice can damage overhead fixed lines and poles, particularly where infrastructure crosses exposed areas.
Extreme heat	High temperatures can cause radio equipment at mobile sites to overheat. Core sites and data centres can also face increased cooling requirements.	Street cabinets and other exposed equipment can overheat, while core facilities may face increased cooling requirements.
Wildfire	Towers, masts and rooftop sites in exposed areas can suffer direct fire damage, while fire can also restrict physical access to sites.	Overhead cables, poles and street cabinets, particularly along vegetation corridors, can be damaged by fire.
Heavy rain	Heavy rain can degrade wireless signals, including through “rain fade”, and can contribute to flooding of ground-level equipment.	Heavy rainfall can lead to flooding and water ingress into ducts, chambers and cabinets, causing equipment damage and service degradation.
Lightning	Elevated towers, masts, antennas and associated electrical equipment are exposed to lightning, which can damage electrical and radio components.	Lightning can damage exposed fixed-network electrical equipment and supporting infrastructure.
Landslides	Geographically dispersed mobile sites can be directly damaged or become inaccessible to maintenance and restoration teams.	Landslides can damage fixed access and backhaul routes or prevent access to affected infrastructure.
Coastal hazards	Mobile infrastructure in coastal locations may be exposed to storm surge, coastal flooding and erosion.	Submarine landing stations and coastal backhaul are particularly exposed to storm surge, sea-level rise, coastal flooding and erosion.
Other severe weather affecting satellite infrastructure	Satellite ground stations, including exposed outdoor antennas and feeder links, can be affected by wind, lightning, snow and heat, while heavy rain can cause signal degradation.	Satellite connectivity can provide an alternative to terrestrial fixed links, but ground equipment remains exposed to severe weather.

Source: Frontier Analysis

Network vulnerability and dependencies

Telecommunications networks are not equally vulnerable. Vulnerability generally increases closer to the access network where assets are more geographically dispersed and often less physically protected. The impact of severe weather on different network assets – and supplier inputs – is described below.

Fixed access networks

High winds can damage overhead cables, poles and attachments, either directly through wind loading or indirectly through falling trees, branches, debris and collapsed structures. Legacy copper networks and aerial fibre networks are particularly vulnerable. Intense rainfall and flooding can overwhelm drainage systems and expose underground ducts, chambers, street cabinets, exchanges and access equipment to water ingress. Water can damage electrical equipment, corrode components, degrade cable performance and delay restoration where pumping, drying or replacement is required.

Mobile access networks

High winds can impose loads on towers and masts, displace antennas or microwave dishes and damage site structures. Even where a tower remains standing, misalignment of antennas or microwave links can degrade service. Lightning can damage electrical and radio equipment and interrupt power supply. Heavy rainfall can affect site access, damage foundations, increase landslide risk and cause localised flooding of equipment shelters or power systems. Snow and ice can increase loading on towers, antennas, poles and overhead power lines, and can restrict access to remote or elevated sites. Severe cold can reduce battery performance, affect generators and complicate refuelling or maintenance.

Backhaul networks

Backhaul and transport networks are moderately vulnerable. Overhead cables and microwave links are more vulnerable to weather events than buried cables. However, operators can reduce vulnerability by using multiple routes and alternative transmission paths.

Core networks and interconnection

Core networks and interconnection facilities are generally less vulnerable to weather hazards because they are usually housed in protected sites with redundancy, controlled environments, backup power and diverse routing. This is due to the operational importance of these facilities: failure of a core network site could cause a significant service outage across a large customer base. However, core infrastructure can still be affected by prolonged power disruption, flooding of buildings or basements, cooling failures, heat stress or water scarcity for cooling systems.

Electronic equipment and heat

Fixed and wireless networks rely on electronic equipment to provide telecommunications services. This equipment is distributed across the network and housed in a range of environments, from data centres, core sites and exchange buildings to equipment rooms and shelters at cell tower sites, outdoor cabinets, distribution points and customer premises equipment. Its vulnerability to heat is therefore not uniform. Equipment in data centres and major exchange buildings is usually protected by active cooling, whereas equipment in outdoor cabinets, tower shelters and small-cell enclosures may have more limited cooling capacity and rely partly or wholly on passive ventilation.

High temperatures can reduce the performance and useful life of electronic equipment used in transmission equipment and batteries, increase cooling needs and increase vulnerability to power system stress or grid outages. In outdoor equipment such as street cabinets, passive cooling systems that were not designed for current or future temperatures are especially vulnerable. Indoors, the operational objective is typically to keep equipment rooms within safe temperature thresholds, below 45–50°C.

70% of surveyed operators experience heatwaves either regularly or occasionally. However, relatively few identified heat as a source of disruption due to the widespread use of cooling and thermal management systems in locations where high temperatures are expected. This means that the main impact of increased heat on electronic equipment is the efficiency of the equipment and the energy demand required to keep the temperature within a reasonable range.

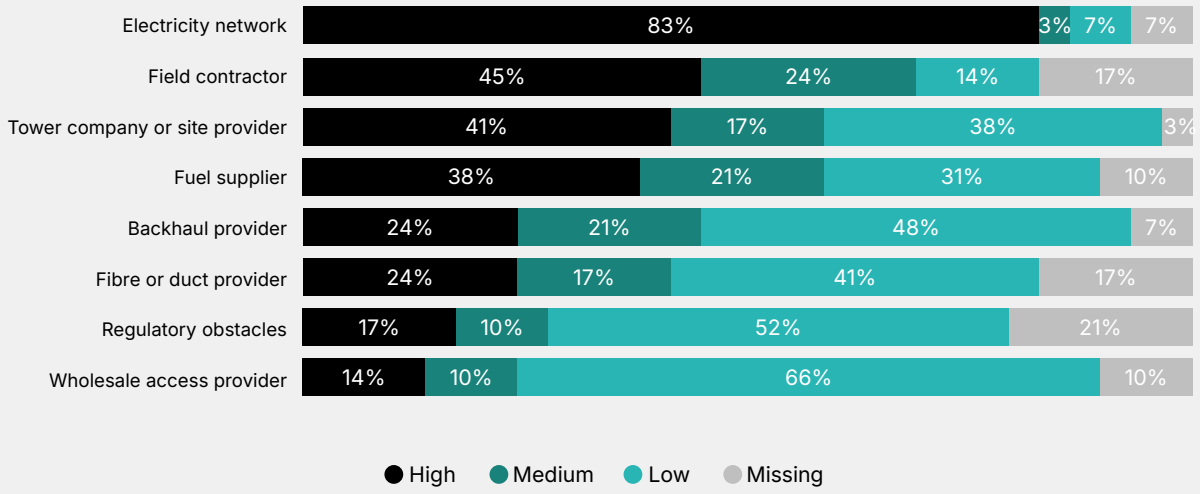
Power and restoration dependencies

Weather hazards can also have indirect impacts on telecommunications networks. These occur where the telecommunications network is disrupted through dependencies on other infrastructure, services or inputs. Most importantly, network elements across all network segments depend on electricity.

All the case studies in this research revealed that power supply and access to fuel are significant risks to service. During the February 2024 Valparaiso wildfires in Chile, almost 300 mobile sites were unavailable at the peak but only 10 were reported directly damaged by fire; most failures followed prolonged electricity cuts and exhaustion of backup power. Flood and storm events in Bangladesh, South Africa and Spain similarly produced a combination of power loss, access restrictions and transmission damage.

In practice, direct and indirect impacts often occur together. A flood may damage a local site, interrupt power, block access routes and prevent refuelling of generators. A wildfire may directly damage sites while also disrupting power supply and limiting field force access. A storm may create network congestion at the same time as it damages power and transport infrastructure. Where backup power is limited, power failure can become the main driver of service disruption, even if telecommunications assets remain physically intact. Figure 4 identifies the prevalence of dependencies that operators view as vulnerabilities for their networks in the context of severe weather.

Figure 4 Dependence on electricity is the clearest systemic vulnerability



Source: GSMA operator survey of 29 operators, consolidated responses dated 20 July 2026; Frontier Economics analysis.

Restoration capability is also a critical determinant of vulnerability. Weather hazards can block roads, damage bridges, restrict access to remote sites, prevent tower climbs, delay fuel deliveries, constrain spare-part logistics and limit the availability of field crews. This means that the duration of an outage may be driven less by the initial technical fault and more by the operator's ability to reach, power, repair and safely recommission the affected asset.

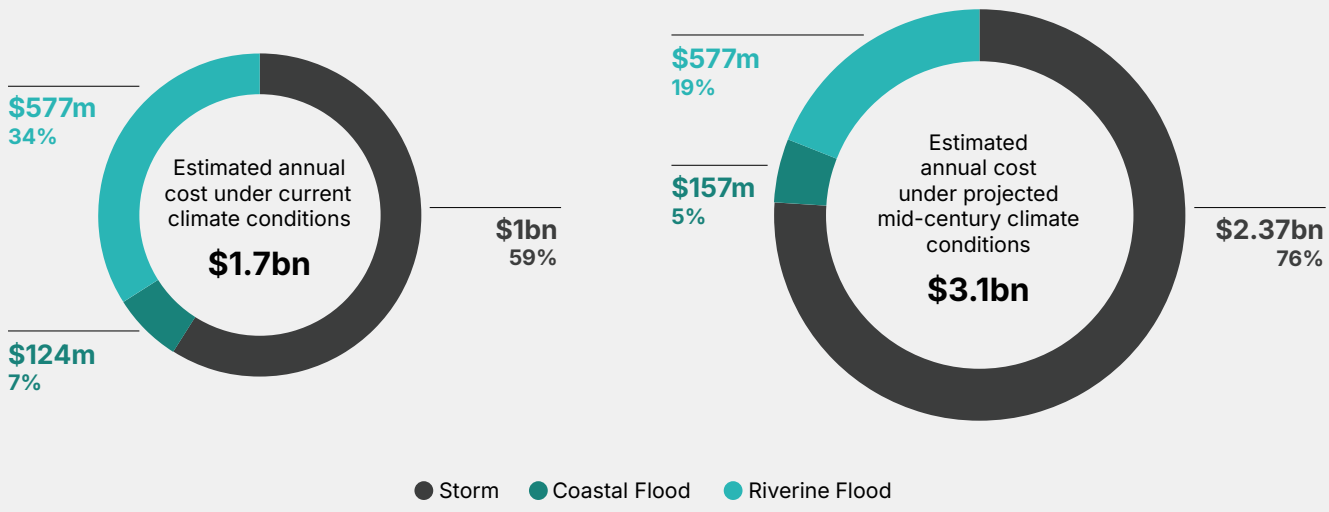
Financial impacts on telecommunications networks

Global costs of severe weather risks

Severe weather events such as storms, flooding (surface flooding, coastal flooding or riverine flooding), extreme heat or wildfire can cause damage to telecommunications infrastructure. Under current conditions, this research estimates that mobile networks face an annual estimated cost of $1.7 billion[11] as a result of damage to cell sites from storm, riverine and coastal floods (including other types of network infrastructure or weather hazards would likely increase this estimate).[12] This represents just under 1% of current global mobile operator CapEx, and approximately 0.2% of global mobile operator revenues.[13] Based on projected mid-century climate conditions, the cost of damage to cell sites is estimated to increase to $3.1 billion per year.[14] This reflects an 80% increase – to 1.6% of global mobile operator CapEx and 0.3% of revenues, respectively.[15]

Under current conditions, $1 billion (59%) is associated with severe storms, while riverine and coastal floods account for 34% ($577 million) and 7% ($124 million), respectively. Based on projected mid-century climate conditions, the costs of severe storms to mobile operators are estimated to rise significantly to $2.4 billion, accounting for a materially larger proportion (76%) of total cost and indicating a material increase in risk, as shown in Figure 5.

Figure 5 Contribution of different weather hazards to expected infrastructure repair and replacement costs



Source: Frontier Economics analysis.

11 Throughout this modelling exercise, "current" climate conditions refers to the general state of climate over the latter part of the 20th century and the early part of the 21st century (approximately 1960–2020). This is based on the time horizons over which the global hazard datasets have been generated.

12 Note that these estimates only include the cost of certain types of severe weather such as storms and flooding (both coastal and inland or riverine) and should therefore be treated as underestimating the true cost to the sector, which can include heat-related damage, weather-related fires or surface flooding. It also excludes damage to fixed networks that can be less readily modelled using public datasets.

13 The GSMA estimates that, collectively, operators invest $200 billion CapEx every year ($1.2 trillion between 2025 and 2030). See: GSMA (2026). The Mobile Economy 2026.

14 Note that the mid-century projections show the risk associated with mid-century climate, as applied to the current network infrastructure. The increase in investment in mobile infrastructure (for example, from denser network architectures) will increase the scale of risk.

15 GSMA. (2026). The Mobile Economy 2026. The report states that global mobile operator revenues were approximately $1.2 trillion in 2025. It also states that global capital expenditure is expected to be $1.2 trillion over 2020 to 2025, implying an average CapEx of $200 billion per year.

This analysis can be extended to fixed networks to generate a high-level estimate of the cost of storm-related damage to fixed network infrastructure. This estimate includes only overhead infrastructure (telegraph poles and overhead lines) given its greater exposure to high winds and potential for damage than underground infrastructure. This indicative exercise suggests that overhead fixed infrastructure faces an annual storm-related repair and replacement cost of approximately $29 million under current climate conditions, increasing to around $81 million under projected mid-century climate conditions.[16] However, this estimate excludes the damage caused by falling vegetation located near fixed infrastructure, which in many countries is more likely to cause damage than the severe weather itself.

The scale of damage to telecommunications networks as a result of severe weather makes it essential for operators to identify the assets most at risk from climate change, both now and in the future, as they can use this data and information to build resilience into their networks. This research supports operators in identifying and estimating, on a consistent basis, the scale of risks they might face.

Regional variation in severe weather costs

Weather hazards vary substantially by location, and the same physical conditions can have different operational consequences in different countries. A temperature that is manageable in one may be dangerous in another if equipment, buildings and operating practices have not been designed for such conditions.

The country case studies conducted for this research illustrate the range of hazards that can affect telecommunications networks:

- In a dispersed archipelago such as **The Bahamas**, a hurricane can simultaneously affect island power systems, ports, airports, submarine cable landing points and fuel delivery. It is not only damage to telecommunications infrastructure that can cause service disruption. The scale and duration of a service outage can also be affected by damage to transport or power infrastructure.
- In **Bangladesh**, widespread flooding can disable many cell sites and make it difficult to rapidly provide fuel to the generators that provide backup power to isolated sites.
- In **South Africa**, chronic grid instability, theft and vandalism affect the resilience of networks to severe weather. Operators noted that theft of backup batteries in remote cell sites also makes mobile networks in those areas less resilient.

Risk assessment therefore needs to consider hazard intensity within the local context. An assessment should include power reliability, access, route diversity, backup duration, site criticality and the capacity of public authorities and suppliers to support restoration.

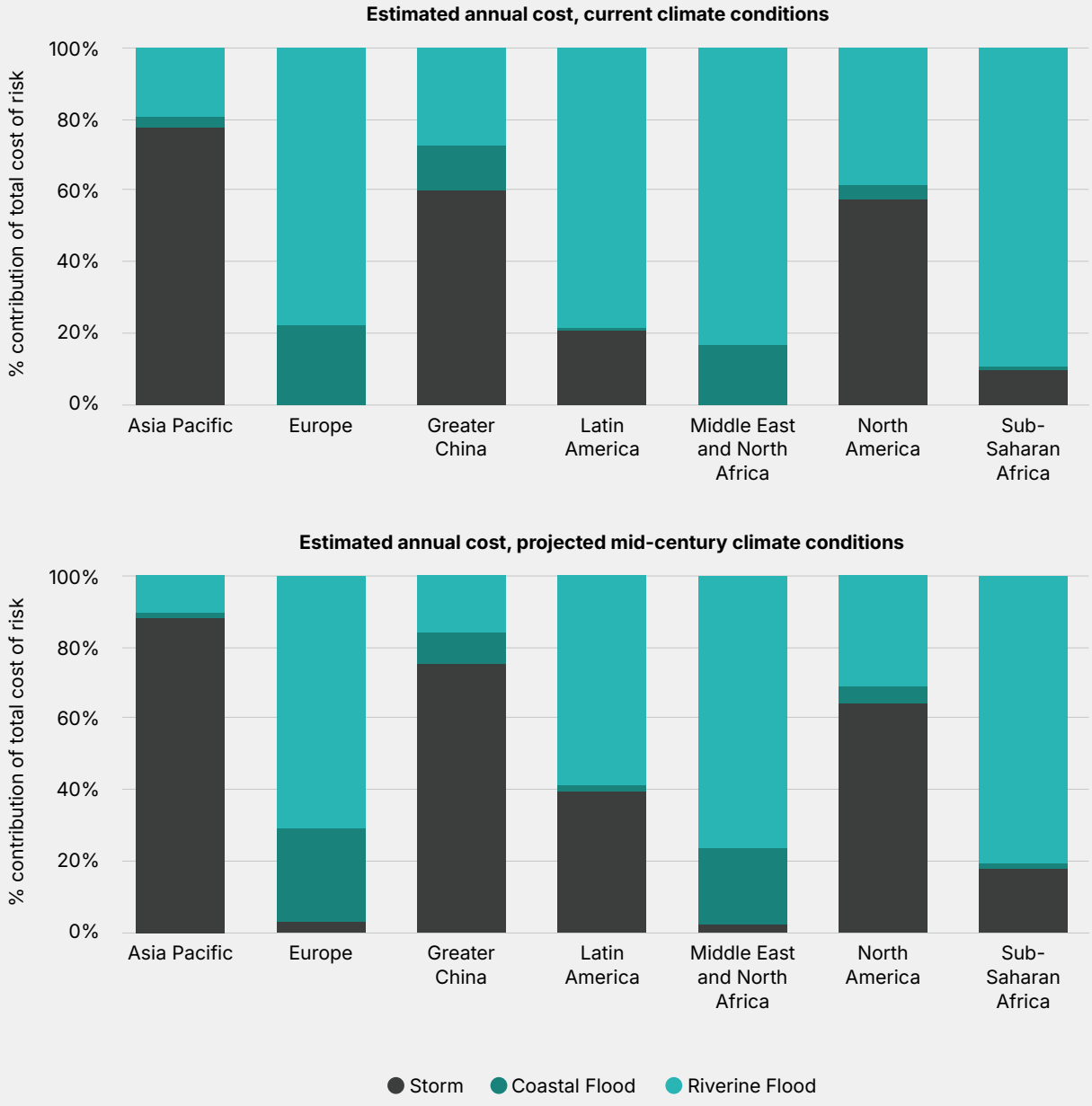
The risks associated with severe weather events are materially different around the world due to the relative risk of different types of weather hazards, as well as differences in repair and replacement costs.[17] Under current climate conditions, riverine flooding represents the greatest relative risk and cost in Sub-Saharan Africa, Middle East and North Africa (MENA), Europe and Latin America. In Asia Pacific, Greater China and North America, the greatest weather risks are associated with severe storms, accounting for 78% ($820 million) in Asia Pacific, 60% ($89 million) in Greater China and 58% ($78 million) in North America.

16 Given the absence of globally consistent geospatial data on fixed network infrastructure, the assessment is a high-level extension of the mobile infrastructure analysis. Specifically, country-level pole stocks are estimated using the UK as a benchmark, scaled according to population and relative fixed broadband penetration. Further, the geographical distribution of poles and overhead lines across windspeed bands is proxied using the distribution of mobile sites established through the geospatial analysis, with published engineering fragility relationships then applied to estimate expected physical damage. These estimates are substantially lower than the corresponding costs for mobile infrastructure, despite the much larger number of fixed network assets, primarily due to the lower direct vulnerability of telecommunications poles and overhead lines to wind (as represented by the engineering fragility relationships used in the analysis). The result is also consistent with experience from recent severe storms in the UK, where official evidence indicates that only a small proportion of poles across the country experienced material physical damage. The estimates should therefore be interpreted as an indicative measure of direct physical damage to poles and overhead lines, rather than the total impact of storms on fixed networks, which can also experience disruption from power outages, falling trees and damage to other network assets.

17 To estimate the total costs at the regional level, the model identified the number of mobile sites at risk of varying severe weather intensities in each country (covered by the dataset) and aggregated this up to the regional level. The total number of at-risk sites were then monetised using the per unit cost estimate from the European Commission's Bottom-Up Mobile Cost Model, adjusted for regional-level price indices to reflect regional variations in the cost of materials and construction. The model employs a region-specific Price Level Index (PLI) from the World Bank. Specifically, the model uses the Construction PLI, which captures regional variations in the expenditure associated with civil engineering works. This is available here: https://databank.worldbank.org/source/icp-2021

As the climate changes, the risk of damage from severe storms will increase much faster than from coastal or river flooding. The annual global cost of severe storms[18] is expected to increase by 138% (from $1 billion to $2.4 billion), compared to an increase of 27% from coastal flooding and a minimal-to-no aggregate change in the cost of river flooding (see Figure 6). As a result, storms will overtake river flooding as the biggest contributor to expected weather-related costs in North America, while becoming a greater risk in all other regions as well.

Figure 6 Contribution of different weather hazards to expected infrastructure repair and replacement costs, by region



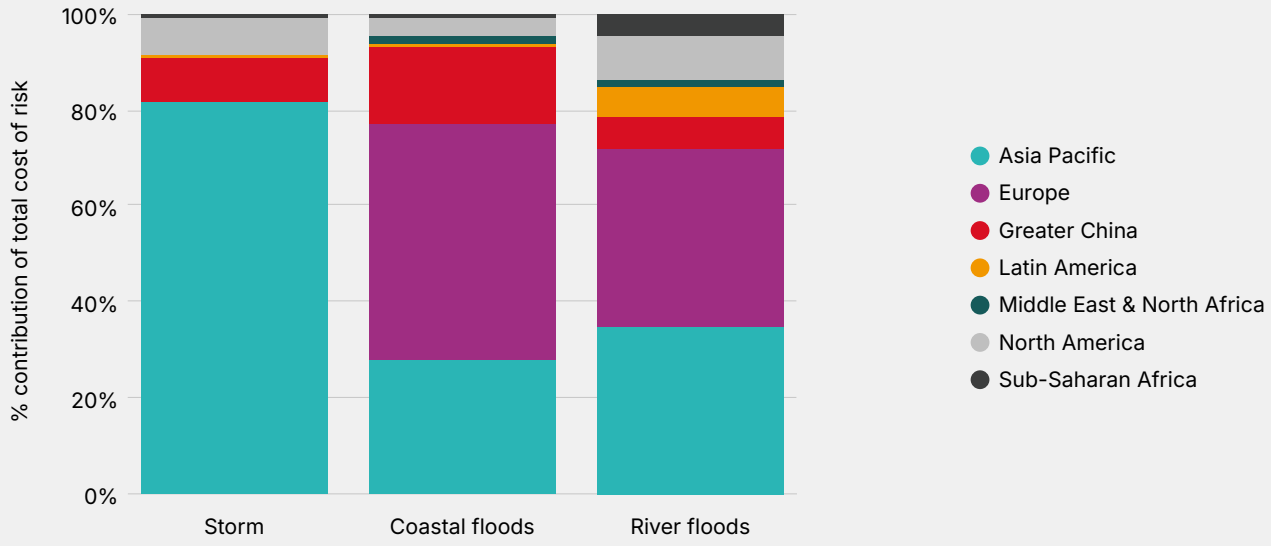
Source: Frontier Economics analysis.

18 Assuming mid-century climate conditions under certain climate scenarios set out in Report 6, Annex 1.

The most significant change in weather-related costs will be in the Asia Pacific region, where the cost of storm damage is estimated to increase from $820 million to $2 billion under projected mid-century climate conditions – a 149% increase. Similarly, Greater China is estimated to face a 135% increase in the costs associated with severe storms, from $89 million to $208 million.

The greatest risk from severe storms is in Asia Pacific while flood-related risk is greatest in Europe followed by Asia Pacific. While the magnitude of the estimated costs is significantly higher between current and projected mid-century climate conditions, the overall contribution of weather-related risk across the different regions is estimated to remain largely stable.

Figure 7 Geographic variation in infrastructure costs associated with different severe weather events, under current climate conditions



Source: Frontier Economics analysis.

Impacts of weather-related network outages

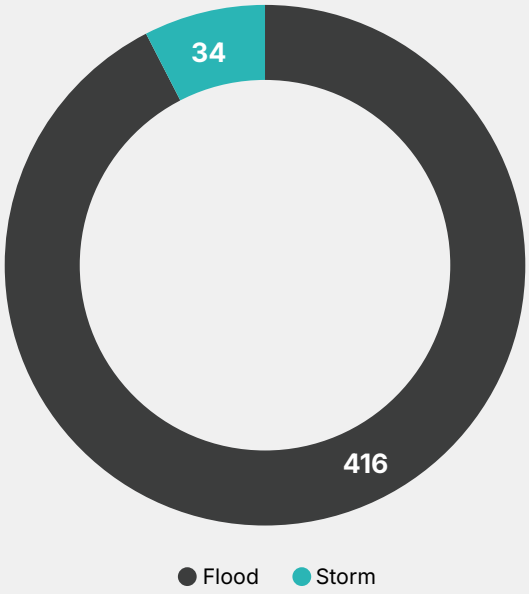
Weather-related network outages

Consumers of telecommunications services face significant costs because of severe weather. When damage to network infrastructure causes service outages, users are unable to use their communication services when they need them most. Between 2022 and 2024 there were, on average, 150 telecommunications outages per year in more than 50 countries occurring at the same time as a severe storm or flood in the region. Based on the scale of these outages, it is plausible to assume that these weather-related outages affected just under 215 million telecommunications service users per year globally. It can also be assumed that climate change will increase the likelihood of service outages over time. **It is estimated[19] that the number of users affected by weather-related outages globally could rise to as high as 280 million a year by mid-century – a 30% increase.**

Most telecommunications outages (92%) were associated with severe flood events, with storms accounting for only 8% of observed outages.

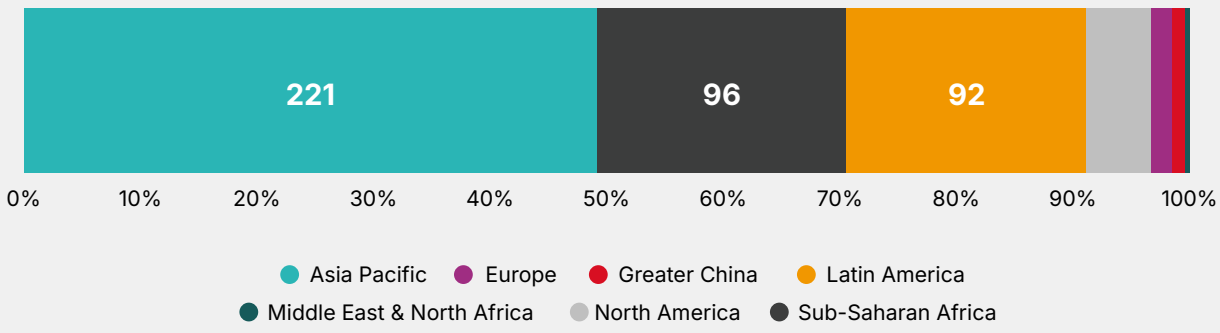
The number of weather-related service outages is significantly higher in Asia Pacific compared to other regions, where approximately 49% of weather-related outages occur. This was followed by Sub-Saharan Africa at 21% (96 outages).

Figure 8 Number of telecommunications outages associated with floods and storms, 2022–2024



Source: Frontier Economics analysis. These estimates should be interpreted as an indication of telecommunications outages caused by severe weather events. For example, the global outage database may not record every disruption, particularly smaller or localised incidents, and the number of users affected and the duration of outages are not observed consistently.

Figure 9 Weather-related outages by region, 2022–2024



Source: Frontier Economics analysis.

19 This is calculated based on the number of (vulnerability-adjusted) mobile sites estimated to be at risk of damage from severe weather events under current and projected mid-century climate conditions. This provides an indicative measure of how service disruption could change as physical climate risks increase or decrease, but assumes that the relationship between infrastructure damage and service outages remains constant over time.

Wider economic impact of communications outages

Communications outages do not just affect telecommunications customers; they also affect the people, businesses and public services that depend on them to function. As connectivity becomes more embedded in everyday life, the potential consequences of weather-related disruption increase.

Mobile and fixed networks now support emergency communications, digital payments, transport systems, healthcare, education, public administration, business operations and access to information during crises.

GSMA research has shown that mobile connectivity underpins the early warning systems, emergency cash transfers, climate insurance and other digital services that help communities prepare for and recover from severe weather events.[20] This means that an outage of the same technical scale can have broader social and economic impacts today than it would have in the past.

For example, Cyclone Gabrielle in New Zealand in 2023 caused widespread power and telecommunications failures across parts of the North Island. Around 80% of mobile cell site outages were associated with loss of power and around 20% with loss of backhaul connectivity. In some affected areas, all three major mobile operators lost coverage. The effects were felt well beyond communications providers. Fire and emergency responders lost communications with some crews and civil defence organisations had to use alternatives such as satellite communications.

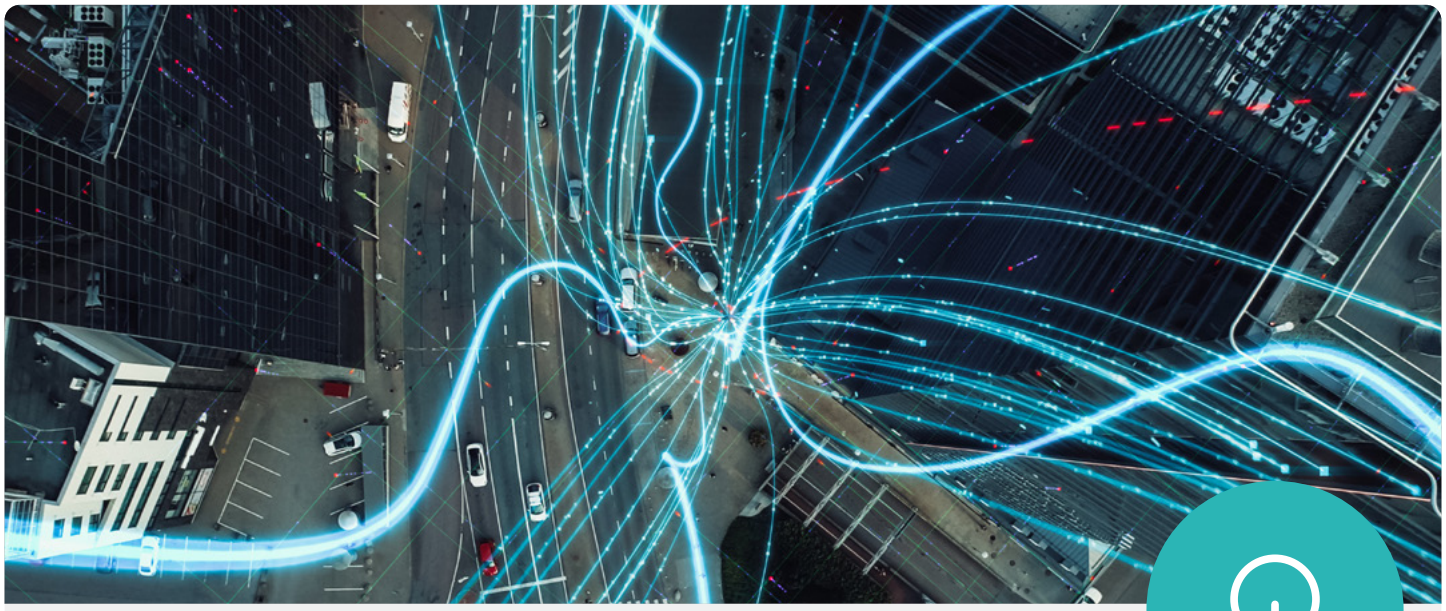
A subsequent review by the New Zealand government found that damage to critical infrastructure, including telecommunications, roads and electricity, hampered coordination of rescue efforts and contributed to the isolation of communities. It therefore recommended that restoration of power and telecommunications should receive greater priority during major emergencies.[21]

The loss of communications services due to severe weather can be significant. The wider economic impact can be difficult to measure as communications outages coincide with other infrastructure damage. However, one study that looked at the economic impact of floods found that a three-day outage in one UK city, which knocked out communications services, reduced the economic output of the area by 10% for the duration of the outage.[22]

Another study[23] found that Hurricane Irma in 2017 led to disruptions across Florida, including to communications services, with 47% of surveyed households experiencing phone or mobile disruption and 69% experiencing internet disruption, with both lasting six days on average. The study estimated that total economic costs reached between $3.7 and $5.3 billion of lost economic output, of which $70–$101 million related to phone outages, and $24–$35 million related to internet outages.



20 GSMA. (2026). ClimateTech Horizons Report 2026, particularly chapter 3, "Early warning systems and humanitarian response", pp. 39–49.
21 Government of New Zealand. (2024). Report of the Government Inquiry into the Response to the North Island Severe Weather Events. See para 230 et seq.
22 Xia, Y. et al. (2019). "Assessing the economic impacts of IT service shutdown during the York flood of 2015 in the UK". Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 475(2224), 20180871.
23 Rafi, S. et al. (2026). "Extreme weather events and critical infrastructure resilience: Lessons from Hurricane Irma in Florida". Reliability Engineering & System Safety, 265, 111471.



Business and industrial activity are becoming more dependent on connectivity, which means the economic impact of severe weather will increase over time.

Connectivity is playing an increasingly important role across the economy. It is embedded in the manufacturing and supply processes of many sectors, and mobile connectivity has become critical infrastructure for digital utilities, transport, public safety and environmental monitoring.[24] Connected sensors, machines and vehicles can enable businesses to monitor conditions in real time, automate processes, remotely control equipment and coordinate activity.

The scale of this change is significant. By the end of 2025, there were more than 1 billion active Internet of Things (IoT) connections globally[25] supporting applications across utilities, transport, industry, cities and infrastructure. Newer 5G capabilities have expanded the range of possible applications, including those requiring higher data volumes, low latency, mobility or more assured network performance.

Connectivity to support industrial applications is becoming increasingly geographically dispersed. Communications are no longer concentrated primarily in offices, homes and other fixed premises. Connectivity is required throughout electricity and water distribution networks, for agriculture or to support drones. This creates a much larger and more geographically diverse set of economic activities that depend on continuous network availability.

This means service outages can have broad industrial impacts. For example, an outage can interrupt monitoring and control systems, prevent connected equipment from operating as intended, delay logistics or inspections or reduce the ability of another infrastructure operator to manage its network. The Organisation for Economic Co-operation and Development (OECD)[26] identifies growing interdependencies between communications networks and sectors such as energy, transport and healthcare, while the International Telecommunication Union (ITU)[27] highlights the potential for digital failures to cascade across sectors.

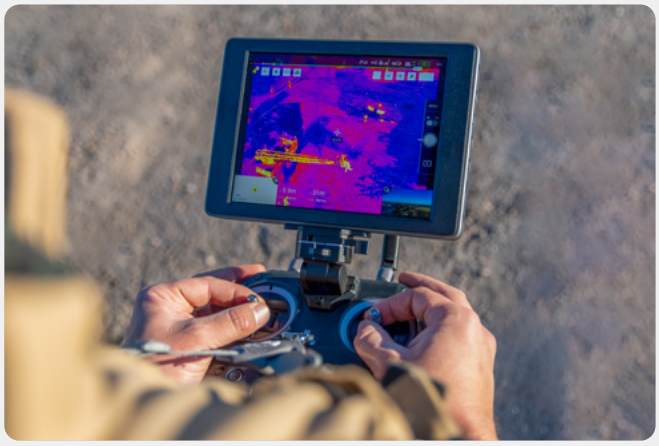
24 GSMA. (2026). ClimateTech Horizons Report 2026, chapter 5, "Cities", particularly pp. 61–63.
25 GSMA. (2026). "A Global Industry Milestone".
26 Cava-Ferreruela, I. and Gonzalez Fanfalone, A. (7 May 2025). "From outage to opportunity: Strengthening the resilience of communication networks". OECD Blog.
27 International Telecommunication Union (ITU), United Nations Office for Disaster Risk Reduction (UNDRR) and Sciences Po et al. (2026). When Digital Systems Fail: An Expert Report on the Hidden Risks of Our Digital World.

Use case 1

Electricity networks

Electricity systems are becoming more decentralised as rooftop solar, wind generation, batteries, electric vehicles and other distributed energy resources connect at different points along the grid. Managing this system requires greater visibility and coordination across geographically dispersed assets. Digital connectivity allows grid operators to collect information from sensors and smart meters, detect faults, remotely manage equipment and coordinate distributed power generation and storage as supply and demand change. The International Energy Agency (IEA)[28] estimates that hundreds of millions of distribution sensors have already been deployed worldwide.





Use case 2

Drones

Commercial drones are increasingly being considered for infrastructure inspection, emergency response, agriculture, construction and logistics. Many of the more advanced applications require drones to operate beyond the visual line of sight of their pilot. Cellular connectivity provides the connection that enables drones to navigate safely while also allowing high-resolution images, video and sensor information to be transmitted to remote operators in real time.

Use case 3

Agriculture

Sensors placed across fields can monitor soil moisture, temperature and weather; connected machinery can transmit operational data; livestock can be monitored remotely; and irrigation systems can respond to information collected from sensors.[29] The ITU identifies precision irrigation, connected tractors, automated livestock systems and drone crop monitoring among the emerging applications of IoT in agriculture.[30] These technologies provide significant improvements in productivity and yield but require dispersed and reliable connectivity.



28 Henriot, P. (12 May 2023). "Unleashing the benefits of data for energy systems". IEA.

29 GSMA research also documents the use of mobile-connected weather platforms, IoT soil sensors, digital agricultural advisory services and mobile financial services to help farmers respond to changing weather conditions and climate shocks. GSMA. (2026). ClimateTech Horizons Report 2026, particularly pp. 26–32 and pp. 36–37.

30 ITU. (2023). ITU-T Y.4000-series: Use cases of Internet of things-based smart agriculture, Supplement 76 (09/2023) to ITU-T Y-series Recommendations.

Conclusion

Weather-related risks are significant and growing. Cell sites face an 80% increase in costs – to $3.1 billion by 2050 – as climate change increases the frequency and intensity of storms and floods.

Outages caused by weather can have major impacts on users and the wider economy, which will only increase as economies become more dependent on communications services. The telecommunications sector must therefore continue to show leadership on climate mitigation activities, which together will limit the worst impacts.

Weather-related risk depends on the severity and likelihood of a hazard, the assets exposed to it, their vulnerability and the consequences of failure. These factors vary materially by geography, network layer and deployment model. Power supply, backhaul and the ability to access and restore sites can be as important as the resilience of telecommunications equipment itself.

The framework and modelling approach presented in this research provides a practical way to identify and measure the impact of weather-related risk (See Report 6, Annex 1).

By combining hazard data with asset locations, vulnerability or fragility relationships and asset values, operators can estimate expected damage and compare how risk varies across hazards, locations and future climate conditions. The modelling illustrates the potential scale of this risk.

Although the estimates are indicative and partial, they demonstrate that weather-related risk can be quantified, is already material and is expected to increase.

The next report in the series considers how regulatory frameworks can support this assessment and how operators can translate identified risks into proportionate prevention, response and recovery measures.

Copyright © 2026 GSM Association