LIFELINES: The Resilient Infrastructure Opportunity

NO BROKEN LINK

The Vulnerability of Telecommunication Infrastructure to Natural Hazards

Himmat Singh Sandhu
Siddhartha Raja

WORLD BANK GROUP

1 2 3 4 19 18 17 16

Cover design by Brad Amburn.

Summary

The global economy is increasingly digital. The internet and other information and communication technologies (ICTs) are changing the way individuals, businesses and governments operate. Their resilience to natural disasters, and their ability to recover in the aftermath, is thus critical to the resilience of the economy. This chapter discusses the impact of climate events on various types of digital infrastructure. It highlights key considerations for governments and digital infrastructure owners to make their infrastructure more resilient, while maintaining affordability of services. We find that digital infrastructure is vulnerable to various climate risks, but that technology choices and network design can improve redundancy and resilience of networks, by design. Certain infrastructures warrant greater ex ante investment in their resilience considering their criticality in the broadband value chain (submarine cables or landing stations) while others could follow repair and recovery options (mobile network antennas, poles, and towers). We conclude with recommendations for the public and private sectors, noting that governments and sector regulators can improve network resilience, and increase coordination given the distributed ownership and governance models in the industry.

Contents

1. Introduction

Information and Communication Technologies (ICT) are deeply enmeshed in the day-to-day activities of individuals, businesses and governments, particularly with the proliferation of the internet and internet-based digital solutions and applications across society.[1] Such an increased dependence on digital technologies and solutions raises questions regarding the resilience, security, and recovery of the underlying infrastructures to various categories of failures—from natural or man-made causes. But protecting digital infrastructure against, or recovering from such failures increases costs, and in the case of a largely private sector-led industry would be borne mostly by users. This Sector Note to the report *Lifelines: The Resilient Infrastructure Opportunity* explore the following policy questions: how does one reconcile the trade-off between *ex ante* cost of building-in resilience, and *ex post* cost of damage and recovery of various digital infrastructure? And how might technological and public policy choices shape this trade-off?

The rapid and expansive digitalization of the economy, enables greater and faster sharing of information driving productivity growth, reduces costs of production, increases access to markets, resulting in an expansion of the traditional economy to a digital economy. Digital infrastructure (including telecommunications networks and information infrastructures such as data centers) has now become a critical input for most industries and socio-economic ecosystems. While its scale, growth rate, and Gross Domestic Product (GDP) contribution are the subjects of debate, there is wide acceptance that such digital infrastructures will underpin future economic growth, in developed and developing countries alike. Their disruption implies economic damage.

In addition to facilitating the daily tasks and operations of individuals and businesses, digital connectivity through telecommunications networks is central to the operation of critical infrastructure and public service delivery. For example, power generation companies and utilities rely heavily on digital connectivity and services in their core operations, particularly for monitoring performance, fault identification and resolution. ERP and CRM systems, now ubiquitous in public and private large enterprises, cannot function without connectivity—and in the case of multinational corporations, without international connectivity between the various operating units spread across the globe.[2]

But this also means that critical infrastructures that were traditionally not connected to or reliant on digital networks are no longer "offline;" their smooth operation is also dependent on the stability, security, and continuity offered by the underlying digital infrastructure. This large-scale

[1] World Bank, "World Development Report 2016: Digital Dividends"

[2] For instance, according to ITU's e-Government index, all 193 UN Member States now have national portals and back-end systems to automate core administrative tasks, and 140 provide at least one transactional service online. ITU E-Government Development Index data, 2018

digitalization means that failures in telecommunication and IT infrastructure will cause failures of the associated critical infrastructure (e.g. power grids, railways, banking, retail services).

While the digital world manifests itself virtually where transactions and information move seamlessly with minimal human intervention, it is built on a foundation of physical infrastructure comprising of cables crisscrossing across the world, antennas, and data centers. Failure of or damage to these physical infrastructures impacts connectivity and other digital services that are critical for individuals, businesses, and governments. While the scale of the impact may vary depending on factors such as the type of infrastructure, location in the value chain, and downstream dependencies, their failure will be felt by many others.

However, unlike other utilities or network-based infrastructure, the ICT sector is mostly privately owned-or-operated globally, with a limited number of countries now having monopolies or dominant State-Owned Enterprises (SOE) in these industries. While the privatization and liberalization of the ICT sector has unleashed massive investment and driven rapid growth in connectivity worldwide, it could also mean that the arrangements for disaster readiness and recovery differ from other network infrastructures or utilities.

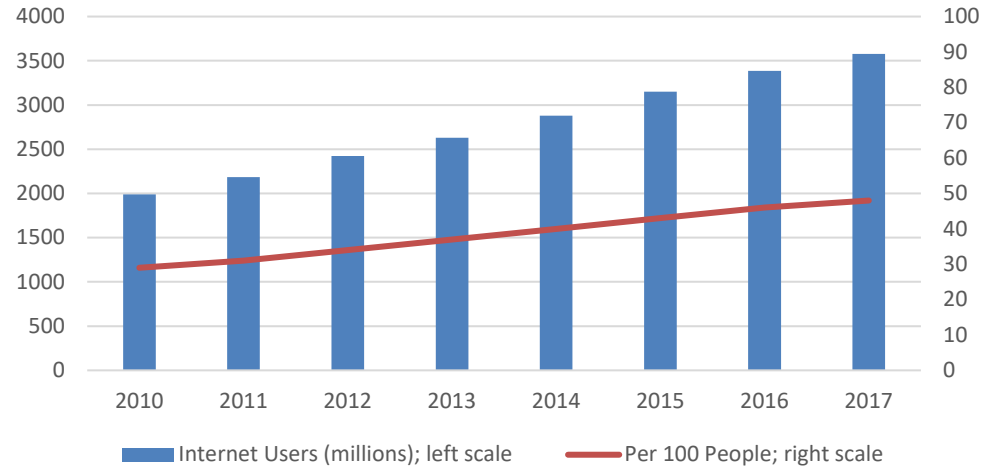
Data on number and intensity of natural disasters suggests that weather related disasters are increasing in number and intensity, making climate resilience and adaptability of society key public policy priorities.[3] Resilience and continuity costs in such cases warrant being shared between the providers and users of services (including the public sector). However, in practice it implies an upfront risk premium often paid by the private sector, with larger scale effects and costs of failures being borne by a much larger set of stakeholders. Furthermore, reconciling the need to expand networks to provide access to broadband connectivity to all at affordable prices, and investing in resilience and recovery efforts is a key challenge faced by the telecommunications operators and governments.

[3] The Economist, "Weather Related Disasters are Increasing," 2017. Accessed from: https://www.economist.com/graphic-detail/2017/08/29/weather-related-disasters-are-increasing

2. The economic importance of digital infrastructure

As seen in figure 1, we have recently crossed a very significant milestone: connecting half the global population to the internet, who are producing hundreds of exabytes of data traffic each month.[4] As more individuals and enterprises come online, and their usage matures, the volume of internet traffic is likely to increase, possibly even after achieving universal connectivity, requiring greater investments in digital infrastructure.

Figure 1: Number of internet users globally



Source: ITU, 2017

Indeed, the rise of digital technologies and the digital economy offer a significant opportunity to unlock new pathways for rapid economic growth, economic mobility, innovation, job creation, and access to services and markets. The internet and digital technologies are expanding access to global markets, changing business models, delivering enormous productivity gains, and expanding access to basic needs and services. In 2016, the global digital economy was worth $11.5 trillion, or 15.5% of global GDP.[5] It is expected to reach 25% in less than a decade, far outpacing the growth of the 'traditional' economy.

Digitalization has thus transformed the way individuals, businesses, and governments operate on a day to day basis. International trade, banking, and finance are entirely digital today, and consumer banking increasingly so. There are approximately 3.24 million ATM machines in the world connected to the internet, serving the global banked population.[6] Communication and social media remain to the most dominant uses of global internet capacity, transforming the way individuals interact and connect globally. Furthermore, governments around the world rely on the

[4] One exabyte is 10 to the 18th power of data, or one billion gigabytes of data.

[5] McKinsey Global Institute, "Digital globalization: The new era of global flows," February 2016

[6] RBR Consulting, "Global ATM Market and Forecasts to 2024," June 2019, London.

internet, digital platforms and other technologies to deliver public services more effectively to their citizens, realizing cost and time savings, and productivity gains. The internet and its services have supported the global technology industry, creating significant value out of data; some digital platforms have global reach and revenues equivalent to countries' GDPs.[7]

[7] World Bank Group, Information and Communications for Development (IC4D): Data Driven Development, 2018

3. The physical foundations of the virtual world

To understand the impact of climate events on digital infrastructure, it is important to understand the risk to the physical infrastructure that underpins it. The large volume of data—including all the internet traffic, financing and banking transactions, and services trade—is carried across the globe over networks of cables, wireless transmitters and receivers, and satellites.

3.1 Networks around the world: Telecommunications

Table 1 highlights the scale of terrestrial connectivity infrastructure around the world. Globally, there are over 13.7 million kilometers of fiber optic or co-axial cables deployed,[8] along key routes between approximately 35,000 key population centers and operated by over 400 entities. Corning—one of the largest manufacturers of optical fiber cable (OFC)—reported delivering its billionth kilometer of optical fiber in 2017, demonstrating the scale of its use.[9] These terrestrial cables are either laid underground, mostly in concrete ducts, or overland on poles and towers. In addition to wired infrastructure, there are nodes such as datacenters and Internet Exchange Points (IXP) that house IT and telecommunication equipment necessary to operate the networks.

Table 1: Length of global terrestrial transmission networks[10]

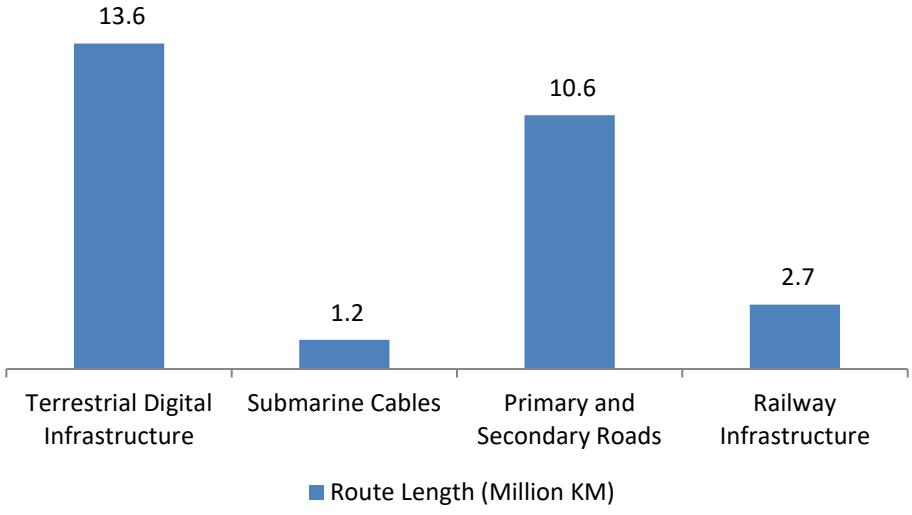
Region	Total Route Kilometers	No. of Transmission Links	No. of Network Nodes	No. of Operators
Africa	5,08,393	5,345	3,567	90
Middle East	4,15,934	1,358	820	40
Asia Pacific	54,05,622	8,739	5,439	92
CIS	12,74,024	2,287	1,201	36
Europe	31,53,815	8,802	5,753	120
Latin America	13,93,403	5,238	3,628	46
North America	15,05,991	2,743	2,005	19
World	**1,37,26,736**	**34,512**	**22,413**	**443**

Source: ITU World Transmission Map, 2019
Note: Lengths do not include last mile connectivity infrastructure—that is, from central "nodes" to the subscriber premises

[8] ITU Global Transmission Maps, 2018.
Note: ITU estimates that the numbers reported capture less than 50% of global terrestrial transmission links, based on response rate of participating telecom infrastructure owners.
[9] https://www.corning.com/worldwide/en/products/communication-networks/products/fiber/milestone.html
[10] ITU Global Transmission Maps, 2018.

The figures above only account only for the major transmission routes around the world—the equivalent of road highways—and do not include lengths of infrastructure deployed within population centers to deliver services to consumers' premises. In addition to the terrestrial networks, there are approximately 1.2 million km of submarine cables connecting continents and islands. [11] Land-locked countries rely on terrestrial infrastructure to bring global internet connectivity inland from submarine cable landing stations, creating trans-continental networks.

Figure 2: Lengths of global digital and land-based transport infrastructure



Source: ITU Transmission Map, 2019; TeleGeography data, 2019; Koks, E., Rozenberg, J., Zorn, C., Tariverdi, M., Vousdoukas, M., Fraser, S.A., Hall, J., and Hallegatte, S. (2019). A global multi-hazard risk analysis of road and railway infrastructure assets. Nature Sustainability.

This physical infrastructure, of varying capacity and ownership models, carries the data at the core of the global digital economy. Figure 3a highlights the total capacity (or bandwidth) of the international connectivity infrastructure—submarine cables, and international terrestrial links—connecting the various regions of the world. Bandwidth connecting Latin America and North America is the highest, followed by Europe and North America, then Asia and North America. Most of the information and thus economic value transmitted over the internet is carried along these routes.

[11] TeleGeography data, 2019

Figure 3a: Connected international bandwidth between regions (Gbps)

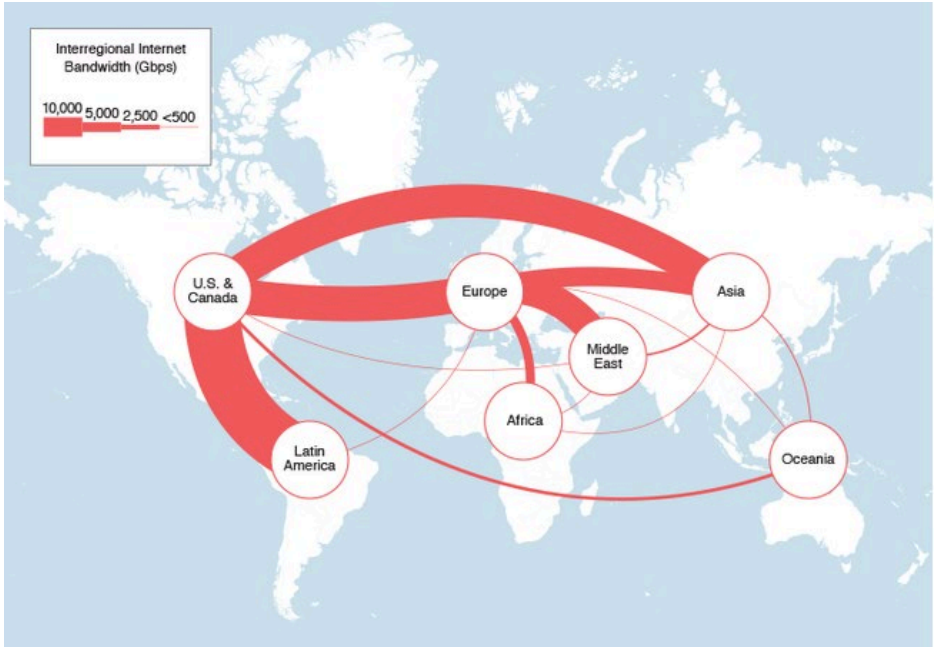


Figure 3b: Global internet bandwidth and traffic trend (2014—2018)

	2014	2015	2016	2017	2018	Change 2014-15	Change 2015-16	Change 2016-17	Change 2017-18	CAGR 2014-18
Internet Bandwidth	127,847	170,297	223,262	290,550	392,976	33%	31%	30%	35%	32%
Average Traffic	34,205	45,692	59,063	75,972	99,632	34%	29%	29%	31%	31%
Peak Traffic	57,354	79,741	100,582	130,953	170,562	39%	26%	30%	30%	31%

Source: TeleGeography data, 2019

Figure 3b illustrates the rapid and consistent growth in bandwidth and traffic over the last 5 years. This requires additional infrastructure, particularly networked infrastructure, to support the growing bandwidth needs of the world. In adding this capacity, the increased climatic risk facing the infrastructure should be a major design consideration, to ensure adequate redundancy while maximizing infrastructure sharing.

Modern Internet Protocol[12] (IP) based telecommunications networks offer a level of resilience by default, which can be further improved with greater physical redundancy—building denser

[12] Internet Protocol refers to a communication protocol in which messages (any type of data—text, audio, video etc.) are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.

networks. In most of the densely-wired parts of the world, there are multiple paths between any two points, and a failure along one pathway may not result in all downstream destinations getting cut off as there could be alternative routes along different alignments. Additionally, since telecommunications is a private sector driven industry, with multiple operators providing services in the same geography, there is a redundancy of services and infrastructure providers along most, if not all, transmission routes.

The shorter lifespan of telecommunications infrastructure compared with other types of critical infrastructure means shorter replacement and upgrade cycles, and lower asset values.[13] The shorter life and rapid rate of innovation also enable infrastructure owners to make technology choices that enable networks to be more resilient. The public sector can also play a critical role in enabling the private sector to periodically upgrade their technology. However, despite these factors, telecommunications infrastructure remains vulnerable to disruptions from acute and chronic climate events.

3.2 Nodes on the internet: Datacenters

Another type of infrastructure needed for networks that comprise the internet are the datacenters[14] where these networks connect, and where content is housed. The datacenters where telecom carriers and content providers exchange traffic or connect are called internet exchange points (IXPs). IXPs enable multilateral connectivity, instead of requiring each operator and content provider to establish bilateral interconnection agreements with others; hence they allow for faster and more cost-effective interconnectivity among telecom operators and content providers. They also reduce costs significantly, particularly for developing countries, allowing them to connect to other operators, saving transit costs in each transaction, rather than sending traffic over international links just to have it return to the country.

Box 1: Datacenters

Datacenters vary in size, depending on their ownership, the purpose or use of the data stored, and the required level of access to this data. For example, any domestic firm in an economy may have a datacenter housing operational data needed for their internal use. This may include such information as the customer database, orders, employee details, or payroll system data, and is not accessible to the outside world over the internet. Such a datacenter may need only a single rack of servers about the size of a closet and can be housed in a single room. On the

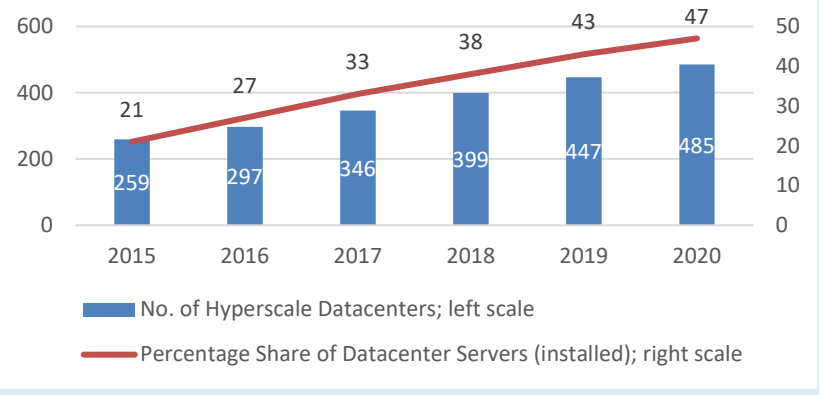
[13] Fu, Horrocks, and Winne, 2018, "Exploring impact of climate change on UK's ICT infrastructure," Infrastructure Asset Management, Vol. 3 Issue 1, Institute of Civil Engineers Publishing.

[14] Gartner defines a data center as the department in an enterprise that houses and maintains back-end information technology (IT) systems and data stores—its mainframes, servers and databases. Physically, it is a location (ranging from an office room to thousands of square meters large facility) that houses servers that require heavy-duty cooling, high-quality poser and backup

other hand, large content providers or global IT companies, require a number of large datacenters with sufficient scalability options to serve an ever- growing market of users of internet-based services. For such companies, the core business is the data housed in these datacenters; they may be compared with large brick and mortar warehouses for traditional manufacturing businesses.

The impact of damage or failure of smaller firm-level datacenters is confined to the owners, and a relatively limited number of users. However, in the case of global IT firms, the impact is substantial, in terms of the number of users, the volume of data housed, and the dependence of the firms and individuals relying on these datacenters in the conduct of their own operations. The scale required of such datacenters has led to a trend toward larger spaces, referred to as "hyperscale" datacenters which offer both space and on-demand scalability.[1] According to Cisco, there were 259 hyperscale datacenters in 2015, operated by about two dozen global IT companies, including Amazon, Google, Microsoft, IBM, and a number of enterprises providing cloud-computing services.[1]

Figure: Number of "hyperscale" datacenters—trend and projections



Source: World Bank Group, Information and Communications for Development (IC4D): Data Driven Development, 2018

3.3 Networks and nodes on the global scale

In summary, it is the 13.7 million km of terrestrial transmission cables, 1.2 million km of submarine cables and their landing stations, over 4 million mobile towers,[15] ~900 IXPs, and ~400 hyperscale datacenters that constitute the global internet used by almost 4 billion individuals, thousands of businesses, and practically all governments globally.

[15] Mordor Intelligence, "Telecom Towers Market—Growth, Trends, and Forecasts (2019—2024)."

Table 2: Summary of global digital infrastructure

Infrastructure	Function	Ownership	Scale
Networked Infra. Cables Antennas Towers	The transport networks carrying global voice and internet traffic	Mostly owned by private sector telecom operators. Alternative owners include utilities, railways and government.	> 13.7 million km. of terrestrial cables, ~1.2 million km. of submarine cables. ~ 4.1 million mobile towers
Nodes IXPs Datacenters Landing Stations	House IT and telecom equipment required to operate the networked infrastructure	Almost entirely private sector, except for government owned datacenters	~ 900 IXPs ~ 400 hyperscale datacenters > 350 submarine cable system with landing stations at every landing point (minimum 2 per cable)

4. Climate impact on Connectivity Infrastructure and Data Centers

For the purposes of analysis of the impacts of climate and other shocks, digital infrastructure can be categorized into the following:

- **Networked Infrastructure**
  - Undersea, or submarine cables
  - Terrestrial cables—underground and overland
  - Wireless transmission infrastructure—towers and antennas
- **Nodes**
  - Landing stations for these submarine cables
  - Internet Exchange Points and datacenters

Here, landing stations could be considered as a form of datacenter. However, they are also generally more secure as they are constructed for a specific purpose, with the protection of the landing submarine cables being a high-priority objective in its design. Table 3 highlights the impact of various climate events on telecommunications infrastructures, based on studies from academia or commissioned by public sector agencies from the UK and USA. The table shows that acute events have a significant impact on almost all forms of infrastructure, with earthquakes (high intensity) being the most destructive across the spectrum of infrastructure elements.

Table 3: Climate events and their impact on telecommunications infrastructure

Infrastructure/ Climatic Event	Inland/ Coastal Floods	Earthquake	Tsunami	Sea Level Rise	High Temp	Water Scarcity	High Winds/ Storm
Submarine Cable (deep sea)	L	H	M	L	L	L	L
Submarine Cable (near shore)	L	H	H	L	L	L	L
Landing Station	H	H	H	H	L	L	L
Terrestrial Cables (underground)	M	H	L	L	L	L	L
Terrestrial Cables (overland)	L	M	L	L	L	L	M
Datacenters	H	M	L	L	M	M	L
Antennas	L	M	L	L	L	L	H

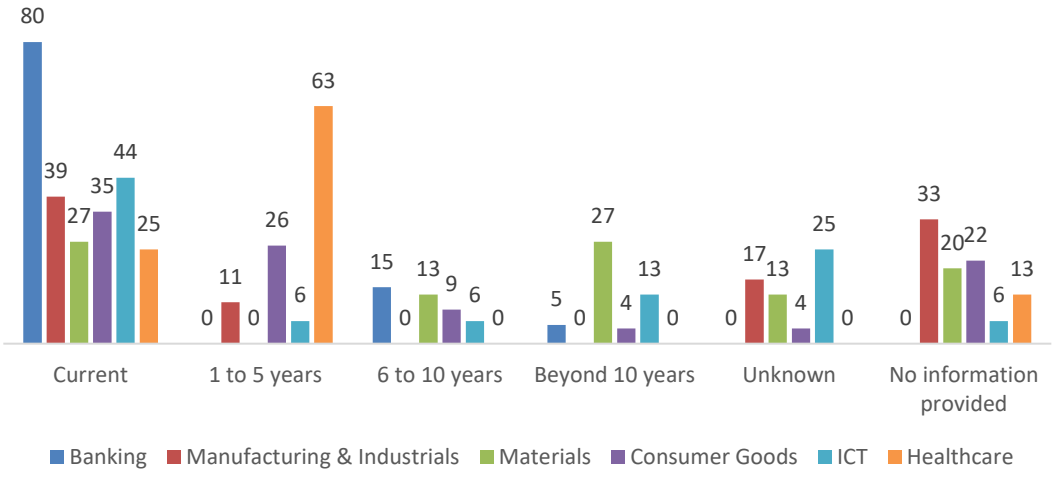
Source: Adapted from: GSA (2014), UK DRO (2018), Fu et al (2016), and Dept. of Homeland Security (2017)

Datacenters and landing stations are particularly at risk from flooding, owing to the relatively large proportion of electronic equipment hosted there and involved in their operations. Submarine

cable landing stations are the most vulnerable to sea level rise, one of the most direct impacts of long-term climate change.

The role played by ICT infrastructure in the global economy as a critical foundational infrastructure for routine operations means that the impact of climate change is already observed. Disruptions to networks have immediate consequences, not only for the owners of the infrastructure but also for users. As seen in Figure 4 below, a survey of the timeframe of climate risks to Standard & Poor Global 100 Index companies reveals the immediate impact of the risks to the ICT sector.[16]

Figure 4: Timeframe of climate risks to Standard & Poor Global 100 Index companies

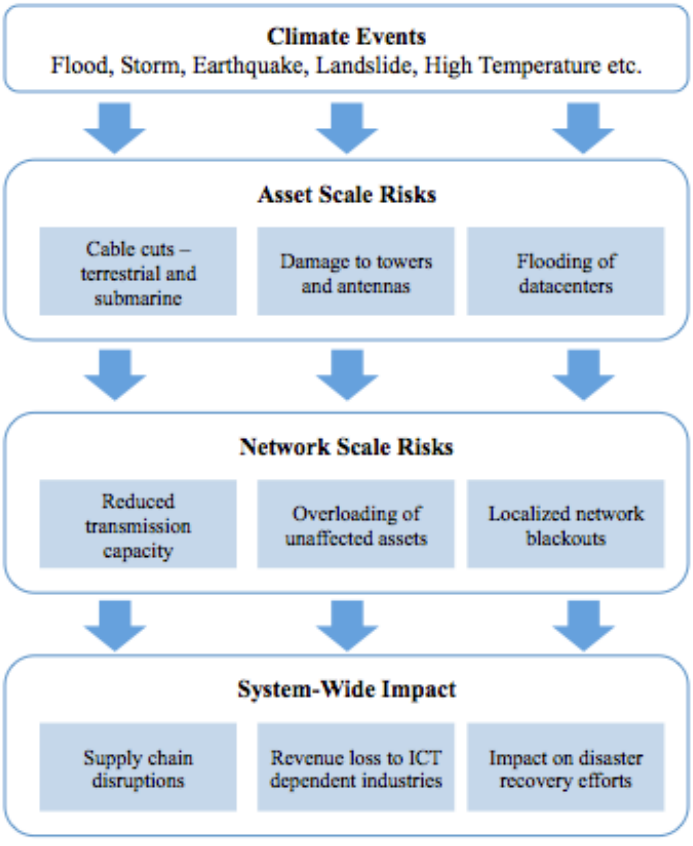


Source: C3ES, Weathering the next storm, 2015

The networked and interdependent nature of telecom infrastructure and services means that risks to telecommunication infrastructure have system-wide impact. Climate events affect specific telecommunication assets, disruptions to which lead to network-wide impacts, such as reduced overall capacity, and overloading of unaffected assets. These network-wide disruptions impact the day-to-day functioning of all industries and individuals dependent on telecommunication services. In addition, they may impede disaster recovery efforts, which rely heavily on the ready availability of communication networks.

[16] https://www.c2es.org/site/assets/uploads/2015/09/weathering-the-next-storm-full-report.pdf

Figure 5: System-wide impact of climate risks to ICT infrastructure



Source: Adapted from Dawson, Richard J. and Thompson, David and Johns, Daniel and Wood, Ruth and Darch, Geo_ and Chapman, Lee and Hughes, Paul N. and Watson, Geo_ V. R. and Paulson, Kevin and Bell, Sarah and Gosling, Simon N. and Powrie, William and Hall, Jim W. (2018) 'A systems framework for national assessment of climate risks to infrastructure.', Philosophical transactions of the Royal Society A : mathematical, physical and engineering sciences., 376 (2121). p. 20170298.

4.1 Impacts along the value chain

Analyzing the climate risks to different types of ICT infrastructures using the broadband value chain can help better understand the impact due to loss of or damage to each type of asset. The broadband value chain comprises of three main segments—

- **First Mile:** International internet connectivity through submarine cables or terrestrial cross-border links
- **Middle Mile:** Domestic connectivity infrastructure linking sources of first mile connectivity to the population centers—mostly cables running along existing connectivity routes (transport and energy)

- **Last Mile:** Infrastructure connecting individuals and premises to telecommunication networks—fiber or cable to the home from local cabinets, mobile towers, Wifi transmitters

The following sections discuss the impact of disruptions to telecommunications infrastructure in each segment of the broadband value chain.

4.2 First Mile Infrastructure

Globally, over 370 submarine cable systems connect to terrestrial networks through landing stations in almost all coastal and island countries. These cable systems are the main arteries of the global internet, and carry the world's information, including virtually all international financial transactions. Perhaps the most immediate effects felt by an economy because of disruptions to submarine cable systems is the impact to international financial transactions, affecting every sector of an economy. In December 2018, SWIFT recorded an average of 34.16 million financial messages per day, with fund transfer volumes more than USD 5 trillion per day, between 11,000 financial institutions across all countries.[17]

Case study 1: December 2006 earthquake in Taiwan, China.

The great Hengchun earthquake of December 2006 on the island of Taiwan, China, and the Luzon Strait provides one of the most severe examples ever of disruptions to submarine cable systems. Submarine landslides triggered by the earthquake travelled over 300 km, and together with the resulting currents, causing 19 breaking points in 7 cable systems. Some of the damage was found at depths of 4000 m, and repairs were conducted by 11 vessels over 49 days.

Internet connectivity was seriously impacted in China; Viet Nam; Taiwan, China; Singapore; Japan; and the Philippines. All of these countries lost a proportion of their international capacity. Financial services, airlines and shipping industries were significantly impacted, and commerce for Taiwan, China, came to a halt. Traffic was rapidly re-routed using undamaged infrastructure, but the pressures on these cable systems resulted in lower quality of service, delays, and failures in from overloading. Following the earthquake, a survey was conducted in China to estimate the impact of the disruption (Beben beschert Rückfall, Telefonzeitalter, Nordkurier, 2006). The results were staggering: it was found that 97% of Chinese internet users faced issues visiting foreign websites, and 57% felt that their life and work was affected.

[17] https://www.swift.com/

These financial transactions and signaling messages are sent over the vast networks of global submarine and terrestrial cables, the importance of which to the global economy cannot be overstated. While satellite communications offer an alternative, and are extensively used in case of disruptions to cable systems, they can only carry a fraction of a country's international traffic: one estimate states that satellites can handle only 7% of the US telecommunications traffic, at a significantly higher cost per Mbps.[18] While the probability of all 35-plus cable systems going offline is small, their economic importance is substantial in almost every sector sectors, from international trade, logistics, shipping and airlines to manufacturing, energy, and the digital sector itself.

While the number and frequency of faults in submarine cable systems is relatively low, parts of the world prone to seismic activity keep submarine cable repair teams busy. Between Taiwan, China, and mainland China, for example, frequent undersea earthquakes result in almost one cable break per week.[19] The presence of a high activity port also makes cable breaks more frequent, mostly due to dropped or dragging anchors hitting garden hose sized submarine cables on the sea floor.

Case study 2: The Great East Japan Earthquake

The Great East Japan Earthquake in March 2011, measuring 9.0-9.1 on the Richter scale, was one of the strongest measured seismic events. The earthquake and resulting tsunami caused damage to a number of submarine cable systems along the Japanese coast. The effects of this disaster on internet connectivity was not as large as that in Taiwan, China, despite the event being of a much higher intensity. The reason for this was the adequate level of redundancy in Japan international connectivity, with submarine cables landing all along the country's coast, in all directions. Unlike the Luzon Strait which has a high concentration of submarine cables, and is the only straight-line path to the island, Japan's diversity of submarine cable system routes ensured overall capacity landing in the country was not significantly curtailed. As a result, while there was some disruption due to cable breaks, international connectivity was surprisingly robust considering the scale of the disaster.

The continuity of operations after such a climatic event demonstrated the importance of well-planned diversity and redundancy of the cable network in times of need. Even with nearly half trans-Pacific cable systems down after the tsunami, international connectivity across the Pacific remained mostly unaffected due to the re-balancing of traffic on unaffected cable systems.

[18] Burnett, Douglas R. "Cable Vision" U.S. Naval Institute Proceedings. (August 2011)

[19] https://www.popularmechanics.com/technology/infrastructure/a8773/protecting-the-submarine-cables-that-wire-our-world-15220942/

However, the disaster did present a unique scenario that was critical in recovery processes. Most of the submarine cable repair vessels in Japan were hit either by the earthquake or tsunami, rendering them unavailable in the immediate aftermath. The event raised awareness for the need to geographically diversify and protect these vessels and avoid losing recovery and repair capability in a time of need.

As Table 3 demonstrates, submarine cable systems are most at risk from earthquakes and landslides on the seabed. This vulnerability also extends to landing stations, but modern construction techniques make the buildings housing these facilities more resilient. However, coastal flooding and tsunamis can cause great damage to landing stations, though, while the off-shore cables themselves may remain protected. However, if either the cable or landing station is damaged, the impact to international connectivity is the same.

One example could indicate the impact of climate and man-made events on submarine connectivity. The most recent submarine cable break to make global headlines happened on January 20, 2019 on the Tonga–Fiji submarine cable that connects the Kingdom of Tonga to the outside world suffered sudden outage. The damage to this cable and the Tonga Domestic Cable was believed to be caused by a ship's anchor and resulted in multiple cuts and the removal of the cable from its trench. The repair process took 11 days to complete, during which the island nation was left entirely isolated from the outside world, with no mobile or internet access.

The USD 30 million cable system supported a significant portion of the country's economy, and the effects of its outage were felt across the board by citizens, businesses and government.[20] Tonga's economy relies heavily on tourism and international remittances. Both sectors came to a near standstill, owing to their highly digitalized nature. Hotel owners and operators could not access booking information and respond to queries from online hotel booking portals, airlines could not take bookings, and families could not receive remittances from relatives working overseas, mostly in New Zealand.

With satellite connectivity as the only other back-up option, the total bandwidth available to country was reduced by a factor of over 200. The satellite link kept essential government services operational, but the private sector and citizens faced the brunt of the outage. Non-essential websites such as social media were blocked to conserve the limited bandwidth available—at a time when over 80% of Tonga's internet traffic was used internationally to access Facebook. The

[20] https://www.aljazeera.com/news/2019/01/tonga-facing-absolute-disaster-internet-cable-blackout-190123030937011.html

country's tourism sector relies heavily on social media, as does the community in staying in touch with its international diaspora.[21]

This case also provides evidence of the vast difference in resilience capability between government telecommunication networks and privately-owned networks. While public networks have adequate redundancy, and prioritize access to back-up connectivity, the private sector relies on its ability to recover rapidly, ensuring continuity of business through commercial agreements with other carriers if necessary. In Tonga's case, however, satellite was the only alternative. The cost of any added resilience or redundancy in private networks will have to be borne by the consumers—the citizens of Tonga. The limited market size does not build a business case for another submarine cable to the islands, and the price implications for broadband services, even if a business case for redundancy was made, are too high.

However, innovations in low-cost remote area connectivity, like Low Earth Orbit satellites, can offer relatively affordable solutions for back-up connectivity. These technologies are still in their nascent stages of commercialization: until they mature, the risk of inadequate redundancy will continue to remain high for small island states and other countries with single sources of international connectivity.

As submarine cable systems continue to proliferate, the possibility increases that these systems will face the challenges of long-term climate change, such as rising sea levels. The telecommunications industry and policymakers need to consider all coastal hazards and plan new deployments of critical international connectivity infrastructure accordingly. Low-cost containerized solutions, for example, can give future landing stations coastal presence for critical ICT equipment, while the cable is backhauled to a more secure location where the majority of the equipment, and thus the landing station itself, is located. These are nascent solutions, but the industry should consider such innovations when making investment decisions with over 20-year outlooks, that factor in climate risks.

A submarine cable landing station is essentially a combination of buildings, underground ducts and conduits, IT and telecommunications equipment, cooling equipment and power back up. Submarine cable systems are built with a 20-25-year outlook, as are the landing stations (see Box 2). However, the equipment within the landing stations may undergo several upgrades and replacement during the life of a cable system.

With the equipment shelter—the landing station building—being the asset with the longest lifespan, upgrades to other elements cannot heavily impact the overall resilience of the landing

[21] https://www.nytimes.com/2019/01/31/world/asia/tonga-internet-blackout.html

station. In addition, since the landing station is a completely immovable asset, it must withstand all possible climate events during its lifecycle.

Box 2: Expected useful life of telecommunications infrastructures[22]

The table below summarizes the expected useful life of various types of digital infrastructures, based on operator reported figures, and industry experience, indicating the period to be considered for planning of resiliency.

Infrastructure Type	Expected Useful Life (Years)
Equipment Shelter (including datacenter shelter)	50
Fiber Optic Cables	20
Conduits	25—50
Poles	28—40
Submarine Cable Systems	25
Areal Cables (all types)	20—25
Switching Equipment (ICT)	10
IP Equipment	3—5
Servers	8
Multiplexers	3

The telecommunications sector also relies heavily on civil works and on the construction industries. These industries, in turn have to keep pace with resilience efforts, in order to ensure the resilience of telecommunications infrastructure. While the use of concrete ducts makes underground cables significantly more resilient compared with simple trenches, improvements in construction and design to make these ducts more resilient to earthquakes and landslides can further improve the climate resilience of the telecommunication infrastructure they carry.

Hence, legislation and regulation in civil works and other related industries thus also play a major role in increasing the resilience of telecommunications infrastructure. Instruments such as construction codes and land categorization can improve the overall resilience of an economy's infrastructure, including telecommunications infrastructure. The interdependencies between the

[22] Adapted from Nevada Department of Taxation (https://tax.nv.gov/uploadedFiles/taxnvgov/Content/Meetings/Expected%20Life%20Study-Telecommunications%20and%20Cable%20Assets.pdf), FCC, operator submitted surveys, and industry experience

critical types of infrastructure in an economy—transport, energy, telecommunication, and water—allow for collaboration on common interests such as the resilience of shared infrastructure, and continuity of business. In this way, non-telecom issues such as construction codes and infrastructure classification can help make landing stations more resilient.

Telecommunications infrastructure, being networked, always has upstream and downstream elements. A submarine cable landing station is perhaps the most upstream element in a country's telecommunications infrastructure. Connectivity from the landing station must be brought inland, or in the case of landlocked countries inland from a border, to population centers. Connectivity must make its way to the closest carrier hotels[23] and IXPs, to other cities, and through last mile networks to subscribers. Having a resilient landing station that can operate under over 6 feet of coastal flooding, does not achieve much if the network beyond the landing station fails in the same scenario. This will be discussed further in the following sections, beginning with the middle-mile.

Case study 3: Intentional sabotage

In 2013, a diver intentionally cut the South East Asia-Middle East-Western-Europe 4 (SMW 4) cable system. The presence of eight submarine cables between Egypt and Europe should have provided sufficient redundancy to prevent significant impact on the country's connectivity. However, four cable systems reported faults or breaks during the same week, resulting in overloads and congestion on the active cable systems. This resulted in Egypt's internet speeds crashing by 60%, with impacts on all telecom operators in the country.

The damage took approximately 20 hours to repair, resulting in immediate economic losses. However, impacts in terms of reduced speed and difficulties connecting to international websites were felt for days. In another case of intentional sabotage in 2007, Vietnamese pirates stole optical amplifiers which left a cable system inoperative for 79 days.

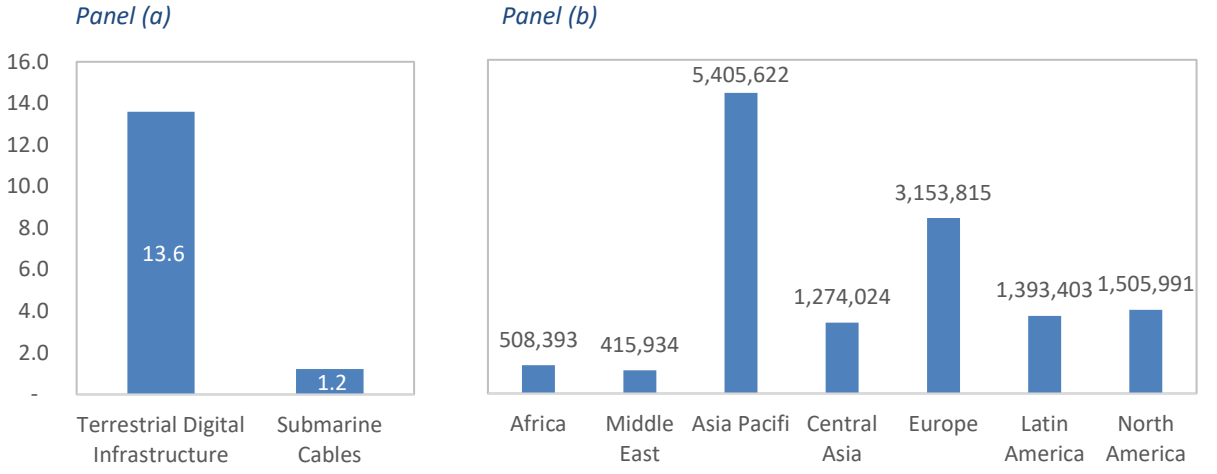
4.3 Middle Mile Infrastructure

The middle mile of broadband networks consists of telecommunications infrastructure connecting population centers within a country, as road highways do. These connectivity routes can also interconnect internationally across terrestrial borders, and form part of the global internet. Countries with well-developed telecommunications sectors have dense middle mile networks, with a larger number of routes, and carriers per route

[23] Carrier hotels, or Meet-Me-Rooms, are locations where multiple telecommunications carriers terminate their cables, enabling bilateral or multilateral connectivity with other carriers present in the location.

Unlike electricity, the transmission routes carry two-way traffic and are now multipath routes by default (due to how IP networks operate), so a break at one point of the network does not necessarily mean everything downstream is disconnected. Large parts of the network can be revived using alternative routes, which may originate downstream from the failure point. However, infrastructure sharing between operators, and with other industries, is reducing this redundancy and increasing risk.

Figure 7: Length of terrestrial digital infrastructure along major routes, and submarine infrastructure (million km), and length of terrestrial digital infrastructure along major routes by region (km)



Source: ITU Transmission Map, 2019; TeleGeography data, 2019

This middle mile infrastructure—consisting mostly of fiber optic cables—is either carried overland on tower, electricity transmission pylons, or poles, or underground in concrete ducts, or via simple trenches. In addition to the cables themselves, a few interconnection points along the transmission routes allow access networks to connect to the internet. These interconnection points house IT and telecommunications equipment and require power supply and back up.

As illustrated in Box 2, the useful life of the cables, and of the passive infrastructure supporting them, is over 15 years, and in the case of ducts, it can be extended further. This segment of the broadband value chain is perhaps the most resilient, and the least at risk. Unlike other utilities, telecommunication networks carry two-way traffic. As a result, an interruption at one point in the network may not impact all downstream elements if alternative routes are available. Additionally, the infrastructure itself is extremely compact—only as wide as a garden hose—and is armored, reducing its exposure to climate events.

Table 3 highlighted the fact that the primary risks to the aerial and underground cables of middle mile infrastructure come from earthquakes, landslides and strong winds. Underground

infrastructure is also at risk from flooding. Infrastructure that runs along coastlines is perhaps most at risk, with exposure to multiple hazards. The availability of hazard maps allows for more effective decision-making about infrastructure choices for new network deployments. The potential resilience of telecommunication networks because of design and technology choices, is most visible in the middle mile, and should be leveraged to the greatest possible extent to build greater redundancy, and thus more resilient telecommunication infrastructure. Telecom operators can use commercial arrangements to build redundancy into their networks and share infrastructure to reduce capital expenses in network roll-out. These savings can in turn be directed towards building the resilience of the most at-risk infrastructure.

In Nepal, for example, the national backbone of middle mile infrastructure underwent significant improvements through investments in ducts, and in the overall strengthening of the infrastructure. As a result, during the 2015 earthquakes, the national backbone remained functional. However, last mile infrastructure took severe damage,[24] illustrating the value of timely and targeted investment in infrastructure resilience, and the consequences of not taking a view of the entire value chain.

Datacenters are an important element of the digital ecosystem, and a vital component of core digital infrastructure. While large hyperscale datacenters are in a limited number of countries, there is a growing trend towards local content, and major digital players like Facebook and Google are placing edge nodes in various parts of the world to serve local markets. As these are the most frequently-accessed websites globally, this results in most of the national internet traffic remaining within these countries where these nodes are located. This may not be the case in several smaller and emerging markets without such nodes.

Industry leaders in datacenter are constantly innovating, with scalability and low energy consumption and wastage as consistent themes. Containerized modules within large datacenters allow for on-demand scalability and efficient energy use. They also facilitate the phased upgrade of technology, and in turn, continuous improvements in resilience. However, most datacenters, such as the ones used by schools, small companies, and remote offices of government agencies are not purpose-built independent facilities. Instead, they are often housed in spare rooms of the infrastructure owner's office premises. This infrastructure is as resilient as the buildings housing it, and the infrastructure of the telecom operators providing the connectivity.

Increases in air and water temperatures affect the output and efficiency of steam and gas turbine-based generators. By the 2080s, under the 4°C climate scenario, this will diminish the effective capacity of electricity networks by reducing the average rating of overhead lines in the distribution network by 6–10%—although the reduction could be up to 27% for some components. These

[24] UNESCAP, Enhancing E-Resilience of ICT Infrastructure, 2015

reductions in performance are smaller than recent historical load growth, which has typically been 1.5–2% per annum.[25]

Case Study 4: Resilience of data centers (Australia, Hotmail, AWS)

In January 2015, on the second hottest day of the summer, thousands of residents in the city of Perth, Australia, found themselves suddenly disconnected from the internet. The Internet Service Provider (ISP) had suffered cooling system failures in part of its data center. While under normal circumstances the failure may not have led to network outages, fears of server failure in the increased heat led the ISP to shut down the servers impacted by the cooling system failure. While annoying and cumbersome for residential customers, the economic impact of a loss of connectivity is felt almost immediately by businesses. Simple tasks such as paying for goods with a credit card become impossible without internet connectivity.

This was not the first, and will unlikely be the last, incident of network or service outage resulting from the overheating of servers in data centers. And as global temperatures rise, the cooling requirements of data centers will increase proportionately, more so as hyper-scale data centers proliferate. In June 2012, an Amazon Web Services data center suffered a power outage resulting from a severe storm in Northern Virginia. The storm led to power outages at the data center, which hosted services such as Netflix, Instagram and Pinterest, all of which were offline for over 2 hours that evening. In August of the following year, a heat spike in certain servers resulting from a failed routine firmware update took down Hotmail and Outlook for 16 hours.

Increasing temperatures and water shortages hit at the core of data center vulnerabilities. The rising temperatures and diminishing water tables under climate change will make cooling increasingly challenging at industrial scales. The Uptime Institute—which tracks data center trends - estimate that companies today can spend almost 80% of cost of running their server on cooling them. A decade ago, cooling costs were close to 150% of computing costs; while this improvement in energy consumption is significant, cooling remains a major challenge.

It is not surprising then, that large new data centers are being established close to the Arctic circle, to keep the servers as cool as possible, reducing energy consumption significantly. Big technology players such as Google are also working on innovations within their existing facilities to improve cooling efficiency. By successfully managing cold and hot aisles in their data centers, Google has dropped cooling costs to approximately 10% of computing cost of their servers.

[25] Dawson, Richard J. and Thompson, David and Johns, Daniel and Wood, Ruth and Darch, Geo_ and Chapman, Lee and Hughes, Paul N. and Watson, Geo_ V. R. and Paulson, Kevin and Bell, Sarah and Gosling, Simon N. and Powrie, William and Hall, Jim W. (2018) 'A systems framework for national assessment of climate risks to infrastructure.', Philosophical transactions of the Royal Society A : mathematical, physical and engineering sciences., 376 (2121). p. 20170298.

While these innovations and investments will continue to strengthen the resilience of data centers, the fragmented ownership and consolidation of resources among a few large players is a challenge.

4.4 Last Mile Infrastructure

Last mile infrastructure refers to the modes of access and supporting telecommunications infrastructure through which end users access connectivity services. These include both wired and wireless access, like traditional cable, fiber to the premises, WiFi, and mobile broadband inter alia. The density of last mile infrastructure follows population density and is highest in urban areas. Telecommunications service providers rely on a combination of aerial and underground infrastructure to extend access to services to their end users, including electricity and telephone poles and underground ducts.

The high density of other types of physical infrastructure makes last mile telecommunication infrastructure more prone to damage. For example, repairs being carried out to an underground water pipe may result in damage to fiber optic cables laid alongside. Similarly, in the event of a natural disaster such as a major storm or earthquake, debris from other physical structures can damage telecommunications infrastructure in its vicinity.

Additionally, since it is the segment of the value chain to which users are exposed, disruptions at this level of the network have an immediate impact and can cause a significant amount of distress in emergency situations. Telecommunication services are vital to disaster response and recovery efforts and play a critical role in the effective delivery of food, water, and building supplies by governments and humanitarian organization.[26] Furthermore, individuals need connectivity services to reach out to family and friends in the aftermath of a natural disaster.

The physical infrastructures most prevalent in last mile access—poles and antennas—are inherently quite resilient and can withstand significant climate pressures. For example, mobile antennae, like the wooden and metal poles used for electrical and telephone wires, can withstand winds up to 250 km/hour. However, falling trees or dislodged debris can damage the infrastructure and cause failures, and are unavoidable. Investments to ensure timely recovery of services in the event of a disaster may thus be more effective than investments in protecting exposed last mile assets. Additionally, there is a dependence on energy supply continuity as well, to power the communications equipment. While most mobile towers and antennas are equipped with backup batteries or generators, damaged roads can make refueling a challenge in the case of extended power outages.

[26] UNOCHA: Information Management: http://www.unocha.org/what-we-do/information-management/overview

In areas under high risk of specific climate events—such as annual tropical storms, or heavy snow—efforts to protect the infrastructure against these specific hazards should be made. Examples of how wireless operators in the US protect infrastructure against an annual storm season provide valuable lessons and are discussed later in this chapter.

Case Study 5: Hurricane Sandy—Damage and lessons learned

Hurricane Sandy demonstrated the impact of acute weather events on telecommunications infrastructure. New York City houses several "carrier hotels", where international carriers interconnect to form the global internet, and this made the impact of a Sandy-scale event potentially catastrophic. Additionally, one of the challenges faced by advanced economies—of upgrading legacy telecom infrastructure—was revealed by the storm.

Several office locations belonging to large operators like Verizon and AT&T flooded because of the storm surge, which also led to power failures, further complicating matters for service providers. Also, as the storage of back-up power and fuel on the top of buildings has been prohibited in New York post-9/11, most back-up power options failed as they were submerged in basements.

The carrier rooms in these office locations suffered catastrophic levels of damage, with miles of copper cables rendered useless. The large amount of copper cables in New York's networks made matters worse, and this highlights the dangers of the delayed replacement of legacy systems in advanced economies: in many developing countries, the initial build-out of networks has leapfrogged the copper generation. Verizon not only lost significant infrastructure in their two 90,000 cubic feet plus vaults carrier vaults in Manhattan, but also across multiple manholes (physical access points for the deployed underground cables) in the city.

During the hurricane, telecom operators had to deploy back-up and restoration equipment which included makeshift mobile towers called Cells-on-Wheels, and the more transportable versions called Cells-on-light-trucks. The storm led to creative problem solving, and collaboration among operators. AT&T and T-Mobile USA joined together in an unprecedented agreement that allowed their customers to roam for free on either party's networks, maximizing their joint remaining coverage.

Verizon estimated the loss at approximately $1 billion and did not see the value in repairing their existing network. Instead they took it as an opportunity to replace the copper networks with fiber optic cables, which are more resilient to water damage.[27] Verizon also undertook several other resilience-enhancing measures to protect their critical infrastructure. The carrier vaults and the fuel storage and pump rooms were made water-tight with submarine doors to ensure continuity of operations. Operators also stepped up efforts to be better equipped to

[27] GSA Climate Risk Study for Telecommunications and Data Centers, 2014

recover after acute weather events, by strategically locating mobile transmission and power sources that can be rapidly deployed.

Case Study 6: Puerto Rico—Making telecom infrastructure more resilient after hurricane Maria

Puerto Rico's infrastructure did not fully recover from Hurricane Irma, with half the island's cell sites still offline a week after the event. But only two weeks after experiencing hurricane Irma, Puerto Rico suffered a near-total loss of connectivity in the aftermath of Hurricane Maria.

95% of cell sites were offline, and it is estimated that 91% of private telecommunications infrastructure was damaged during the hurricane. Operators reported that 80% of above-ground fiber and almost 90% of last mile fiber was destroyed in the hurricane as well. Until January 2018, it is estimated that 60% of the online telecommunications infrastructure had to rely on diesel generators. Also, only one submarine cable supported the island's international connectivity at the time. In all the island sustained an estimated US $ 1.5 billion in damage to telecommunications infrastructure alone.

The near-total collapse of telecommunications also impacted emergency response and recovery coordination efforts: callers struggled to get through on the 911 emergency line, and response teams could not be easily dispatched.

Limited maintenance of telecom infrastructure was highlighted as a root cause of its lack of resilience and the extent of the damage it suffered. The extensive above-ground deployment of fiber optic and landline cables (as opposed to using underground ducts) was also identified as a major cause of the extent of network outage and infrastructure damage. Inefficiencies in emergency response were also identified.

The recovery plan for the island highlights such activities as public and private sector capacity building as pre-requisites for creating the right enabling environment for investments in innovative critical infrastructure—including telecommunication infrastructure. Some of the key steps being undertaken are:[28]

- Building GIS capability to allow for improvements in public safety, disaster recovery, emergency response, community planning, infrastructure deployment planning etc.
- Consolidating or upgrading existing Land Mobile Radio Systems supporting microwave wireless communication
- Implementing standardized power backup
- Developing communication networks in rural areas

[28] Post Hurricane Maria reconstruction plan—Puerto Rico

- Upgrading 911 services to current technology
- Procuring mobile emergency communication equipment
- Improving connectivity to mainland USA through submarine cables to increase redundancy
- Streamlining processes for permitting and rights of ways authorizations for telecom network deployment
- Performing periodic site structural audits of Government telecom towers

Technology choices can also play a key role in enhancing the resilience of telecommunication infrastructure. The continued use of legacy copper wires in New York possibly resulted in greater damage than if the infrastructure had already been upgraded to fiber optic cables, which are better insulated from water damage by design. Similarly, innovative technologies are becoming increasingly relevant to service recovery efforts. Advances in low-cost, long-range drone technology have enabled the deployment of unmanned drones to provide coverage over disaster hit areas. Transportable antennas, towers on wheels, and other modular transmission solutions are also being mainstreamed by mobile operators globally. The public sector can play a key role in facilitating the testing and adoption of such innovations through incentives, through potential shared ownership models, and through emergency authorizations to deploy such technologies in post-disaster recovery efforts.

Box 3: Infrastructure sharing

The telecommunications sector has a long history of sharing infrastructure, and more recently, of sharing services. Mobile operators have recognized the benefits of sharing towers with each other, leading to reduced costs and faster network deployment. Additionally, telecom operators also engage in commercial agreements to lease capacity from each other to reach new markets along routes where their own infrastructure is not deployed.

In recent years, telecom-ready infrastructure in other sectors—particularly energy and surface transport—have also been utilized by telecom operators to deploy networks. With civil works constituting between 60—90% of the cost of deploying fiber optic networks, the business case for sharing these costs within and between sectors is clear. And in their efforts to extend access to connectivity to rural and remote areas, governments globally are promoting such infrastructure sharing as a cost reduction mechanism.

However, in countries with lower density of telecommunication infrastructures (for example fewer routes and operators per route), limited infrastructure sharing can also contribute towards reducing the redundancy of telecommunication networks.

Policymakers and sector stakeholders should thus consider how sharing can help physical redundancy of telecommunication networks, with cost reduction and resilience enhancement.

5. Avoiding broken links

Telecommunications infrastructure, as described earlier, includes a variety of assets with a wide cost range. For example, fiber optic cables, the actual superhighways of the internet, cost a fraction per kilometer when compared to roads or railways. While the telecom and IT equipment housed in data centers and submarine cable landing stations, mobile towers and antenna are significant capital expenses, the total cost of digital infrastructure in a country will still be much lower than that of the total electricity or surface transport infrastructure. Being networked infrastructure, it allows owners and regulators to identify and rectify points of failures, enabling steps to be taken in advance to mitigate against increased exposure by establishing redundancies, or increasing resilience.

However, there are also physically exposed assets, such as antennae, that may not warrant investment in ex-ante resilience, and can instead be easily replaced in the event of a disaster. Investing in the protection of these assets would not yield proportional returns, compared with an investment in backups or restoration preparedness.

As a result, owners of telecommunication infrastructure need to consider three types of resilience investment decisions:

- investment in ex-ante resilience;
- redundancy; and
- investment in restoration and post-disaster back up.

The choice of the strategy is driven by the economic value of the infrastructure, and the role it plays in the network. A submarine cable system landing station is an investment of both high economic values, and of high value to the network. Such an asset would warrant ex-ante investment in its resilience. Datacenters also fall under this category of telecommunications assets, particularly hyperscale datacenters that cost millions of dollars in capital expense.

Middle mile infrastructure offers the opportunity to create multiple pathways between population centers in a country. Well-functioning telecommunication sectors tend to have competitive domestic wholesale markets, with multiple players and routes. This creates opportunities for commercial arrangements to create redundancies, both for service providers and their users. While the sector is highly competitive in general, telecommunications operators collaborate through commercial negotiations to establish redundant routes, and are able to cope with faults and failures, with minimal impact to subscribers, by routing traffic through these alternative routes. This segment of the broadband value chain demonstrates the inherent resilience of telecommunication networks, and this “comparative advantage” of the sector should be leveraged to maximize its resilience. Governments can also use regulatory tools to facilitate the above through cost reduction, pro-competition, and transparency regulatory actions.

Private sector players are increasingly investing in recovery and service restoration preparedness to counter the impacts of acute climatic events on last mile infrastructure[29]. The last mile of the broadband value chain often suffers the most damage, and in the event of a disaster, citizens, businesses and governments feel the impact directly through lost communication services. The recent cases of hurricane damage in Florida and Puerto Rico have demonstrated both the devastating impact on last mile networks, and the possibility of rapid recovery if preparations are adequate (or indeed, its converse).

The telecommunications sector faces unique challenges when compared to providers of other types of infrastructure, and these challenges add to the complication, and thus the risk, of investment decisions in infrastructure resilience. Despite being a largely privately owned and profitable industry, the telecommunications sector continues to play a utility-like role in an economy, delivering critical infrastructure to people and businesses. Most providers of critical infrastructure are either partly or fully government owned, or significantly regulated. They do not experience the challenges of fragmented ownership, competition, and lack of public sector funds typical of the telecommunications sector.

Some of these sector-specific considerations that eventually impact investment decisions in resilience are discussed below.

Private and distributed ownership: Telecommunications infrastructure globally is largely privately owned, and in the case of submarine cable systems, often owned by multi-country consortiums. Because of this distributed ownership (including across jurisdictions), information on the existing resilience levels of infrastructure can be incomplete, and decisions to invest in resilience become challenging. Differing ownership structures and management priorities can also result in varying levels of resilience of infrastructure, with little or no outside visibility on the subject, except because of mandatory regulatory reporting.

To cope with this issue, the datacenter industry has evolved internationally in a culture of adherence to standards. These standards and certifications serve an important marketing role for the industry, and their providers demand commensurate prices. In the case of telecommunications access networks, individual consumers are the primary market, and competition is driven by network coverage, price and service offering, not by the resilience of the operators' infrastructure to shocks. However, due to the increasingly important role connectivity plays in the economy, institutional subscribers demand certain service levels and assurances of business continuity and enforce them through Service Level Agreements (SLA) with their connectivity providers.

[29] Refer case study on preparedness for hurricane season in the USA

Reconciling resilience needs and the affordability of connectivity services: With broadband connectivity now considered a necessary pre-requisite to compete in the global economy, significant efforts are being made to achieve universal access to broadband services by 2030. The affordability of services is a significant barrier to achieving this goal; accordingly, the UN Broadband Commission for Sustainable Development recently reduced its target for affordability of services from 5% to 2% of GNI per capita for an entry-level broadband plan.[30]

Telecommunications operators face a difficult challenge in reducing prices, particularly given the stiff competition in the market. Making their digital infrastructure more resilient may involve additional investment that does not offer immediate returns. Private sector operators often cite the lack of a business case for investing in resilience, and the lack of standardized approaches across the industry to estimate the risk, magnitude, and likelihood of natural disaster impacts makes the production of such business cases and collaboration among operators more difficult. In the meantime, pressures to compete in the market, and to onboard new subscribers generally receive a greater share of investment and attention.

Cross-sector interdependencies of the telecommunication sector: The utility-like role of the telecommunications sector has been highlighted earlier in this Note. One would be hard-pressed to think of sectors that do not have a digital component in their value chains (See Box 4). However, some cross-sector relationships take primacy due to their criticality. For example, the telecommunications sector cannot function without power to run the equipment making up the digital infrastructure, and the sector's customers cannot use services without access to electricity either. Power outages are common during climate and other shocks and preparing for these is an important consideration. While generators and battery back-up are available at all critical telecommunications infrastructure sites, they still need to be accessible to be supplied with fuel if the initial stock expires. In the case of severe flooding, it may be impossible to replenish the necessary supplies of fuel or batteries.

While the public sector directly supports resilience and recovery efforts in the case of most other critical infrastructures, this could be difficult to institutionalize in the case of the telecommunications sector. However, the public sector can encourage or incentivize investment in resilience by the private owners of infrastructure as part of their upgrading and expansion plans. The case of the telecommunications sector has thus demonstrated that the public sector can play an enabling role in private sector-led growth, filling investment gaps when necessary. The same approach could extend to building resilience of telecommunication infrastructure.

[30] https://broadbandcommission.org/Documents/publications/wef2018.pdf

Box 4: Cross-sector interdependencies

ICT has evolved from being a sector making an independent contribution to an economy to one that also boosts the contribution of each of the other sectors in that economy. Fu *et al* highlight cross-sector interdependencies and the risks that arise from these. Below are some examples of certain categories of sectors or systems that depend on ICT:[1]

- **Business-as-usual:** Customer transactions (including electronic banking); Staff-to-staff communication (e-mail, phone call, videoconferencing); Financial management; E-commerce; Ticketing and billing systems; Customer/passenger information systems; Healthcare provision; Automated Teller Machines
- **Control Systems:** Traffic signaling; Traffic management; Navigation (waterborne, satellite- and land-based); Vehicles—road and rail; Aircraft and marine vessels; Rail signaling; Air traffic management; Supply chain management; Logistics (dispatch and delivery of goods); Real-time delivery management and reporting; Supervisory Control and Data Acquisition (SCADA); Remote management of pumps and switches in network; Water distribution; Energy generation and distribution; ICT network management
- **Incident Management:** Policing, fire and rescue, ambulance; Transport delay rectification; Natural emergencies response; Man-made emergencies response

The criticality of telecommunication services demonstrates the knock-on effects of failures in network connectivity. Additionally, the dependence of telecommunication service providers and users on electricity and other infrastructure also creates challenges during natural disasters. The reliance of each contributing sector on the others' business protocols and climate resilience efforts creates a chain of dependencies, with effects throughout the ecosystem in case of a single element failing.

International best practices have shown that policy leadership in raising awareness and taking a system-wide view of the resilience of critical infrastructure achieves results. Economies facing the challenge of replacing legacy infrastructure are particularly at risk of suffering significant loss to their telecommunication infrastructure in the case of acute climate and other events: the damage to legacy copper cabling during Hurricane Sandy is a case in point. In Nepal, by contrast, investments in reinforcing backbone networks paid dividends during the 2015 earthquake, when most of the damage to telecommunications infrastructure was limited to last-mile assets. Below are some case studies highlighting other resilience efforts undertaken globally.

Case Study 7: Braving the Atlantic storm season

The hurricane season 2017 was a particularly devastating for the Caribbean and southern United States, with the US Virgin Islands and Puerto Rico suffering near-complete devastation of critical infrastructure, and a number of mainland areas in Florida and neighboring states

experiencing storm related losses. The relative impacts on the islands and on the mainland US, provide a useful illustration of the importance of building the resilience of infrastructure against such events.

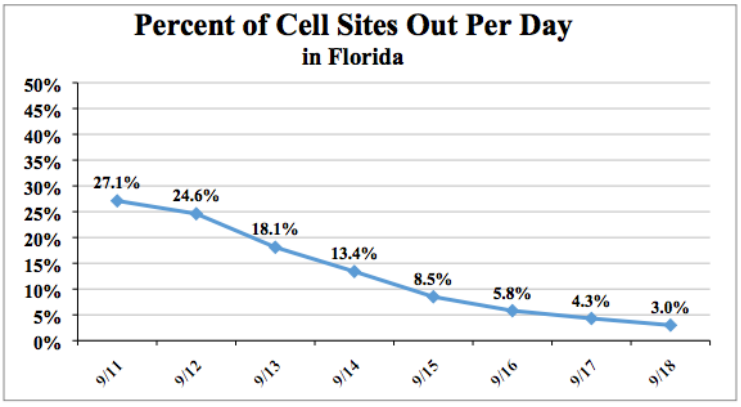
In the US, the annual recurrence of hurricane season has prompted significant resilience and recovery preparation by telecom operators, and public sector-driven warning, preparation, relief and recovery efforts have resulted in improved resilience and faster recovery. While last mile infrastructure can be made resilient through certain good practices, violent climate events are likely to cause damage to exposed assets such as towers and antennae, and even underground assets like ducts and cables. Operators need to be prepared and have the resources and assets in place to restore services as quickly as possible. This has led the telecom sector in the USA to mainstream innovations such as Cells-on-Wheels, mobile power backup, and distributed fuel storage systems inter alia in.

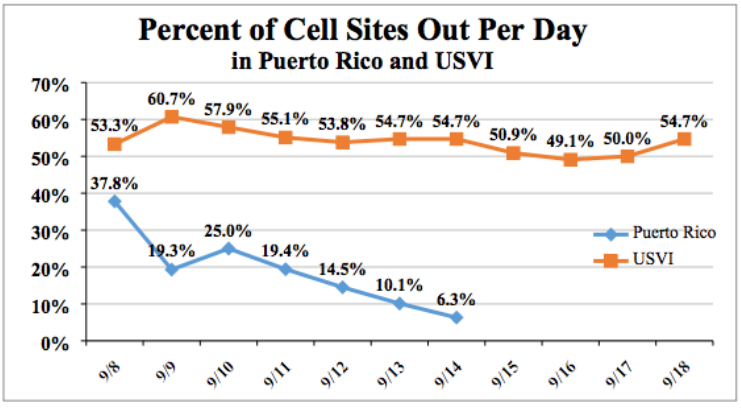
Public agencies and operators have also increased awareness efforts to prepare their clients and the general population for potential disruptions, providing tips to minimize impact. The Federal Communications Commission (FCC), the telecom sector regulator, also awards short-term Special Temporary Authorizations (STAs) to restore communications in the aftermath of disasters. In 2017, FCC awarded almost 1,000 STAs in the recovery efforts after hurricanes Harvey, Irma and Maria.

The FCC was also proactive in the activation of emergency response and disaster recovery teams in anticipation of hurricanes. For example, FEMA and DIRS were activated for all hurricanes, and significant outreach efforts undertaken to ensure smooth reporting, information sharing and coordination in continuity of operations, restoration and recovery efforts.

Years of iterative preparation resulted in rapid recovery times in hurricane affected parts of mainland USA. However, the US Virgin Islands were unfortunately severely battered by both Hurricane Irma and Maria in a short time period, leading to near complete loss of telecommunications infrastructure. The same was the case for Puerto Rico in the aftermath of hurricane Maria (see case study on Puerto Rico's response to the hurricane), and both territories experienced near black-out for extended periods of time. By contrast, Florida saw 97% of cell sites back online within a week of the hurricane, which had initially caused 27% of these sites to go offline.

Figure: Percentage of cell site out-of-service in Florida, US Virgin Islands (USVI) and Puerto Rico due to Hurricane Irma





Source: FCC report on 2017 hurricane season

6. Portfolio of Measures and Recommendations

The private sector's motivations to invest in resilience are driven by (i) economic incentives to reduce the risk of their investments by mitigating against climate risk; (ii) serving their client's needs, adhering to Service Level Agreements, and upholding their reputation; and (iii) serving the interests of their area of operation by providing a critical service during emergencies.[31] This last motive ensures the public good provided by this privately-owned infrastructure, acknowledging its mission-critical nature for an economy.

The importance of telecommunications infrastructure, particularly submarine cables and landing stations is also increasingly highlighted in discussions around national security. In addition to action taken on cybersecurity and the protection of critical online infrastructure, the physical protection of the internet's underlying infrastructure should also be a policy and industry-wide priority.

The private sector, as owners of much of the infrastructure, will need to take the lead in investing in resilience of their assets, while the public sector plays the role of a facilitator and develops the right enabling environment for investment in resilience of critical infrastructures. The public sector's policy leadership on climate resilience of critical infrastructures is necessary in driving actions across sectors, and fostering a holistic approach to climate adaptation, resilience, and disaster recovery. Given below are some high-level recommendations for the building of greater resilience in global telecommunications infrastructure.

1. Create awareness of climate risks to telecommunications infrastructure, and the importance of the infrastructure's resilience to chronic and acute climatic events

Literature on the topic of the climate resilience of ICT infrastructure highlights low levels of active discussion on the topic. With the intensity of severe climate events increasing over time, infrastructure owners and policymakers need to focus attention on at-risk telecommunications infrastructure. Individual enterprises have taken the lead and made investments in infrastructure factoring in the impacts of climate change, and the needs of the infrastructure. Facebook's decision to reduce cooling costs by developing a hyperscale datacenter in the Arctic circle with access to adequate cold water, is evidence of individual enterprises taking the lead in making the internet more resilient. However, there is limited awareness and dialog in the sector, and within countries, regarding the climate risk to ICT infrastructure.

[31] Biagini B., Miller, A. (2013), "Engaging the Private Sector in Adaptation to Climate Change in Developing Countries: Importance, Status and Challenges", Climate and Development, Vol. 5, Issue 3, pages 242-252

Public Sector Recommendations:

- Conduct **periodic infrastructure climate risk assessments** and include telecommunications infrastructure as critical infrastructure for these assessments. Overall, a greater number of countries are conducting climate risk assessments for various sectors—sixteen G20 countries have multi-sector national climate risk assessments for infrastructure, as reported by OECD. However, only a limited number of countries conduct ICT and datacenter specific climate risk assessments. While certain governments may have their own private telecommunications networks, the importance of communications services to the economy and citizens today, means that assessing the vulnerability of privately-owned networks is as important. International connectivity, in particular submarine cables, takes priority in this respect since it can be a major choke point for countries with limited international connectivity. Both public and private sector stakeholders should take a collaborative approach towards understanding the risks as well as efforts and investment involved in mitigating against them and building resilience in high-risk areas. Lessons from the aftermath of Hurricane Sandy in New York and the 2017 Atlantic hurricane season demonstrate the success of adopting a holistic approach to response and recovery. However, it is now necessary to extend these efforts to resilience as well and continue to move towards a proactive stance towards climate risks as opposed to reactive.
- Conduct periodic **private sector consultations** to understand concerns and challenges faced by the private sector and inform the development of an enabling environment that builds a business case for the private sector to invest in resilience and continuity of business. Additionally, the private sector is also equipped to develop and adopt the latest innovations in infrastructure resilience, early warning, and recovery. Periodic consultations can help the government ensure these innovations have the necessary support to be deployed in emergencies.

Private Sector Recommendations

- **Assess current climate exposure to assets** across the value chain and identify vulnerabilities. Telecommunication networks follow population centers, and vulnerabilities identified one operator can very often be shared by other operators, or utilities. As a result, opportunities to share risks and costs may emerge, and have a positive impact on the business case for investment in infrastructure resilience.
- **Make institutional and private users aware of the steps being undertaken to make the infrastructure behind the services received by them more resilient.** The datacenter industry uses security and safety certifications and audits to attract users and demand commensurate premiums. As greater awareness of the need for the resilience of telecommunications infrastructure spreads, it can also be leveraged as a differentiating factor between operators.

2. Design and upgrade for resilience

Lower asset cost, relatively shorter asset life, and rapid rate of technological change allow for frequent upgrades to telecommunications infrastructure. Additionally, generational change in telecommunication technology often requires replacement of legacy systems, such as in the case of migration from metal cables to fiber optic cables for transmitting data. In both situations, as well as in the case of new asset deployments, infrastructure owners have an opportunity to assess and enhance resilience of the asset. The public sector can also ensure each law, policy or regulation being drafted that may have an impact on network infrastructure, should factor in resilience investment facilitation related considerations.

Public Sector Recommendations

- **Update policies, laws and regulations that impact deployment of telecommunications infrastructure to include resilience building measures.** These measures may be included in areas such as building construction codes, asset specifications, and land categorization. In addition, the application of international standards should be promoted in equipment, civil works, and network planning, inter alia. The public sector can also set benchmarks for the industry using standardized resilience requirements in the public procurement of connectivity and other digital services.

- **Standardize resilience enhancing elements in fully or partially publicly funded infrastructure.** In the case of Nepal, the concerted efforts to strengthen middle mile networks using conduits and addressing vulnerabilities in the years leading up to the 2015 earthquake paid dividends as the middle mile infrastructure went largely unaffected. Last mile infrastructure—mostly aerial—was severely impacted.

Private Sector Recommendations

- **Include climate risk in business cases and investment decisions made by owners of telecommunications infrastructure.** Climate risks are being factored into the investment decisions of several industries. The geographic spread and exposure of a lot of telecommunications infrastructure increases the risk, or reduces the lifespan, of investments made in the expansion of broadband networks, particularly with increased climate risks. Business cases in the telecommunications industry need to actively factor in climate-related risks, including those that may potentially arise later in the lifespan of the assets. All new network deployments, replacements and upgrades provide opportunities for the assessment of climate risk that can negatively impact returns on the investments, or increase risk, which in most cases is transferred to the users as a cost.
- **Upgrade to IP based communication:** IP based communication allows for greater resilience by default because of the technology itself.
- Identify assets most at risk based on climate risk assessments and prioritize actions to enhance their resilience. Perform a **cost benefit analysis of various climate-proofing**

options for the assets and develop a phased approach to resilience building. This can allow for better management of working capital, and smoothen the need for resources used for enhancing resilience of infrastructure over time.

3. Coordinate actions

While functioning as foundational infrastructure for all sectors of the economy, the telecommunications sector is itself highly dependent on energy, road transport, and in the case of datacenters, water. Interruptions to these critical infrastructures impacts the functioning of telecommunications infrastructure, as highlighted in various case studies in this chapter. During acute climate events, all these infrastructures are exposed and at risk simultaneously. The interdependencies between these sectors, and the roles they play in emergency response and recovery efforts, make it necessary to coordinate effectively between the various stakeholders. Governments, as the drivers of emergency response and recovery efforts, can benefit from taking a holistic approach to resilience, response and recovery, particularly in high-risk areas. Similarly, private sector stakeholders can save costs, strengthen their infrastructure, and increase returns on investments through greater and more effective coordination of infrastructure deployment, resilience investment, and recovery efforts.

Public Sector Recommendations

- **Adopt a holistic approach to infrastructure resilience, disaster preparedness, emergency response, and recovery.** Such an approach should be focused on ensuring the greatest possible availability of critical infrastructures—transport, telecommunications, energy, and water. Sensitizing stakeholders involved in emergency response and recovery efforts to the various interdependencies and common pinch points can help reduce the impact of climate events on infrastructure and make these efforts more effective. A coordinated strategy, with well-defined roles and procedures, can better utilize limited resources, and ensure the continued availability of interdependent infrastructure to limit the knock-on effects of its failure.

- **Develop open data and information sharing platforms to enable sector stakeholders to effectively prepare for, and recover from, climate events.** In addition to sharing data, the various stakeholders can also share expertise. For example, the public sector may have access to localized hazard maps for climate risks, while operators have data on infrastructure locations, and back up resources at sites, but neither may have the human capital to analyze the data. This may come from a university or climate study institute that contributes to or has access to the platform.

Private Sector Recommendations:

- **Build on existing collaborations among telecom operators, and between sectors, to reduce cost of network deployments and build the resilience of shared infrastructure.**

A cost and risk sharing approach, while easily applicable to new shared deployments, such as ducts and conduits, can also be used to upgrade existing shared infrastructure. With utilities such as electricity, water, gas and telecommunications often serving the same households, opportunities to co-invest in resilience building efforts can yield a greater rate of return of investment for all parties involved.

- **Extend the culture of co-operative competition in infrastructure among telecommunications operators to sharing data and disaster recovery resources.** There are many instances of mobile operators allowing free domestic roaming on their networks for subscribers of other operators in the aftermaths of disasters. Such efforts can be expanded to proactive collaboration in readiness, and the sharing of investment in recovery equipment. Leveraging each other's' sites and locations across cities can help restore connectivity faster in the event of a natural disaster. Additionally, the private sector can greatly assist resilience, response and recovery efforts

4. Mobilize financing for increased investment in infrastructure resilience

Reconciling the need to increase affordability while investing in climate resilience is a big challenge for the sector, particularly given the public good provided by communications services, and their criticality to the global economy. While government communications networks may have adequate physical redundancy and are not concerned with the financial viability of these investments, private sector operators often rely on commercial arrangements to build in redundancy into their networks. They need to pass on the cost of investments in resilience to the users of their services. With increased climate risk, the private and public sectors will need to mobilize investment to strengthen existing networks, and ensure new deployments adhere to certain climate resilience standards.

Public Sector Recommendations:

- **Provide viability gap funding for investments in resilience.** The public sector has used innovative models to support sector financing in the past, particularly to work towards extending access to connectivity in rural and remote areas. In such cases, **viability gap financing** makes a viable business case for private sector investment in low-revenue areas of the country. Such programs can also be used to finance viability gaps in telecommunications infrastructure resilience. Models such as reverse auction subsidies, public procurement of services to provide an anchor client to telecom service providers, and universal access funds have been utilized successfully across the world, and similar models can be devised to make investments in climate resilience of infrastructure more viable or include them in network deployment.

- **Promote adoption of international standards for telecommunications infrastructure**. It may be necessary to support operators with economic incentives to adhere to the standards, undertake periodic audits and assessment for compliance, and facilitate dispute resolution.

Private Sector Recommendations:

- **Undertake periodic cost-benefit analysis of climate proofing exposed assets to make financial provisions for resilience efforts**. Additionally, due to the geographical spread and highly exposed nature of telecommunication assets, climate risk should be included in operators' contingency planning. These activities can help operators understand the scale of investments necessary to increase climate resilience of their infrastructure, and plan for them in a phased manner.
- **Monetize enhanced resilience and certifications**, like the datacenter industry. While individual subscribers may not see the value in paying a premium for a more climate resilient network, institutional customers may see value in doing so from a continuity of business perspective. Enhanced resilience of infrastructure can also become a differentiator for operators in what is a very competitive sector.

In conclusion, considering and investing in the resilience and recovery of global digital infrastructure should be a public and private sector priority. Given the distributed ownership and varied governance and operating models across the industry, there is a need for greater coordination of resilience and recovery efforts between the wide range of stakeholders in the sector. Reconciling the costs of increased investment in resilience, and the need to improving affordability of broadband services is a key consideration, particularly for the public sector. This may require targeted regulatory interventions to incentivize more resilient technology choices, network design, and infrastructure deployment/ upgrade, as well as measures that reduce the time and economic cost of investments. To undertake the above actions, there is a need to create greater awareness and understanding of the impact of climate-related risks to digital infrastructure, and possible collaborative solutions that benefit all stakeholders—infrastructure owners, users, and governments.