Climate Risks Study for Telecommunications and Data Center Services

REPORT PREPARED FOR THE GENERAL SERVICES ADMINISTRATION

Global Science Solutions

Prepared by:

RIVERSIDE
global science solutions

ACCLIMATISE

RIVERSIDE TECHNOLOGY, INC. ■ 2950 EAST HARMONY ROAD, SUITE 390 ■ FORT COLLINS, CO 80528
TEL. (970) 484-7573 ■ FAX (970) 484-7593 ■ www.riverside.com

Climate Risks Study for Telecommunications and Data Center Services

REPORT PREPARED FOR THE GENERAL SERVICES ADMINISTRATION
By Riverside Technology, inc. and Acclimatise

Lead Authors

Peter Adams
Acclimatise

Jennifer Steeves
Acclimatise

Contributing Authors

Brian Ashe
Riverside Technology, inc.

John Firth
Acclimatise

Ben Rabb, PhD
Acclimatise

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

Executive Summary

Telecommunications and data centers are key utilities sectors that facilitate the functioning and connectivity of the United States economy. Disruptions in the ability to communicate or access information severely inhibit governments, companies, and citizens, and in periods of disaster or extreme events, this inability to communicate puts national and human security and business value at risk. Climate variability and change may threaten the infrastructural integrity and productivity of these critical sectors, increasing the number and severity of disruptions. Extreme or unusual weather can lead to cascading impacts felt across sectors and borders. However, despite the importance of these sectors, the climate risk they face is poorly understood. Even less understood are climate risks to the supply chains both sectors rely upon. This report presents an initial step toward understanding how climate change may disrupt these sectors, how resilience can be fostered, and recommends next steps.

Climate risk is business risk. The assets, equipment, and operating procedures of these sectors were designed to function within specific climate and environmental conditions. Climate change (which can include both incremental changes as well as extreme events) can impact the operating parameters and enterprise supply chains, causing impacts to telecoms and data center companies and their customers. Impacts may result in changes to functionality, quality of service, return on investment, business continuity, and cost, in addition to cascading impacts on the diverse customers that rely upon them. Value protection strategies are required to address these risks.

Climate change poses both dramatic and subtle challenges. Extreme weather events, like Hurricane Sandy in 2012 and the Thai floods in 2011, dramatically show the potential economic cost of climate change in the near term. However, cumulative or gradual climate impacts are less likely to be studied due to failure to spot the signals if operating performance gradually deteriorates, uncertainty of the timing and magnitude of impacts, the absence of stakeholder consensus in the wake of an extreme event, and the short-term decision-making time frames of many businesses. These impacts can lead to increasing costs and reduce the expected lifespan of assets and infrastructure. There is great need for businesses to understand, assess, and prioritize different kinds of climate risks.

Global supply chains present a range of global climate risks. The supply chains that provide goods and services in support of both these sectors face a wide range of potential impacts from climate change. However, this complex network means that climate impacts to one part of the supply chain in one region of the world can have consequences for other parts of the supply chain in other regions of the world. A single climate event can have compound effects, with a range of direct and indirect impacts across sectors and in many countries. However, the literature scan contained in this report demonstrates that little attention is currently paid to the range of climate risks in the supply chains supporting these sectors. This report presents supply chain maps for the telecommunications and data center sectors as a first step to assist in understanding how and where climate impacts may present material risks and new opportunities. Further research to address this gap will increase not only the climate resilience of these sectors, but also the resilience of their diverse customers reliant on information services for their functionality, capacity, operations, and security.

Infrastructure risks are better understood than supply chain risks. While climate risks to such vital supply chain inputs as electricity appear significant, the focus in the small but growing literature on telecommunications and data center climate risks focuses on infrastructure to the near exclusion of enterprise supply chains. This gap needs to be addressed to determine the relative significance of climate risks to the network of inputs, parts, and services that support information and communications technology (ICT) sectors.

A trend toward sharing and consolidating infrastructure reduces redundancy and contributes to climate risk. Recent legislation allows companies to share telecommunications and data center infrastructure but this, along with government plans to consolidate data centers, reduces redundancy across the network and generates single points of failure.

Some solutions exist, but more work needs to be done. This report highlights a number of suggested adaptation options from around the world, including some case studies of early implementation actions by telecommunications companies to build resilience. However, many adaptation actions remain untested or poorly documented. It is critical to explore adaptation solutions, first by framing climate risks in the language of business and then collaborating with key experts representing the engineering, technological, and operational aspects of both sectors to discuss climate impacts in the short and far terms.

This report leads to a number of key recommendations:

- **Frame climate risks as business risks** using the language of business, not science, and contextualizing climate risk from the perspective of private sector companies, their customers, investors, and regulators.

- **Plan for both a changing climate baseline and for climate extremes**. Successfully addressing climate risk requires careful attention to subtle impacts (e.g., the cumulative impact of increasing sequences of warmer than average days on wired telecommunications) as well as to the effects of extreme storms.

- **Build awareness of climate risks before disasters strike**. Working with stakeholders to build consensus and collect the information each offers is to effectively build resilience.

- **Conduct direct consultations with the private sector** to understand their needs, strengths, and weaknesses, as these stakeholders know the business, sites, and technologies best and can help build understanding of what would happen under likely climate scenarios.

- **Thoroughly assess climate risk of both telecoms and data center sectors**, informed by consultations with experts and stakeholders. This will allow for the prioritization of risks to both sectors according to their relative consequence and likelihood.

- **Require federal service providers to demonstrate climate resilience** in all procurement processes, with suppliers required to undertake a climate risk assessment and demonstrate how their products and services will continue to meet required contractual and serviceability performance standards.

- **Elucidate, test, and document adaptation options as value protection strategies** in both sectors, as many of these strategies and fixes remain prescriptive, undetailed, and/or untested.

- **Assess operating headrooms for key assets in both sectors** to understand the functional thresholds for critical assets in a changing climate, which will assist in identifying and prioritizing risks, planning operational maintenance, and informing future capital expenditures.

- **Assess both sectors within the context of their asset lifetimes**, with climate risk assessments scaled to the life cycles of assets and equipment. Though lifetimes are short, assets must be robust during their useful lives.

- **Include telecoms and data centers in the fourth National Climate Assessment,** alongside other key sectors already represented.

- **Provide guidance on SEC material risk disclosure.**

1. Introduction

Riverside Technology, inc. and Acclimatise were commissioned by the GSA to study climate risks to the telecommunications and data center services sectors.

The US has the largest telecommunications market in the world, and it is projected to experience rapid domestic growth of around 3.7 percent each year, reaching $721 billion by 2015 (Verizon, 2011). As defined by the North American Industry Classification System (NAICS), the primary purpose of organizations in the telecommunications sector is the operation of and/or provision of access to facilities for the transmission of voice, data, text, sound, and video. The sector includes establishments that provide telecommunications and related services, namely telephony, including Voice over Internet Protocol (VoIP); cable and satellite television distribution services; Internet access; and telecommunications reselling services.

There are four industry sub-sectors:

- Wired
- Wireless
- Satellite
- Telecommunications resellers

The first three are comprised of transmission facilities and infrastructure operators that own and/or lease assets in order to provide telecommunications services. The fourth consists of providers of support activities and telecommunications reselling services. It also includes providers of many of the same services provided by the first three groups that are not telecommunications carriers (US Census, 2014). Telecommunications services are essential to the effective operation of the global economy, benefiting every other industry. In an increasingly digital world, they also have vital social functions to perform. They are touted as helping to address greenhouse gas emissions and other sustainability issues by offering low impact alternatives to travel. Telecoms also provide critical tools for managing emergency responses during periods of disaster or extreme weather.

According to the NAICS, the “data processing and hosting service sector” provides specialized hosting activities, such as web hosting, streaming services, application hosting, application service provisioning, and time-sharing of mainframe facilities to clients. Data processing establishments provide complete processing and specialized reports from data supplied by clients or provide automated data processing and data entry services (US Census, 2014). Whether hosting or processing, data centers increasingly represent key nodes that are vital for maintaining the successful operation of today’s global communications infrastructure. At the same time, uptime expectations from customers continue to grow (Ricardo-AEA, 2014). A unique selling point of data centers is that customers who utilize them to store data are promised safety from data loss in times of extreme weather. ‘The Cloud’ is actively being promoted as a tool to combat weather disruption where it is suggested that with data stored virtually in a secure, purpose-built data center, businesses can be confident that their information is highly secure regardless of what the weather conditions are (Sourcing Focus, 2014). Of course, this is only true if the data center has been designed to be climate resilient along with all its essential supplies and services. Addtionally, it also requires a trained and resilient workforce.

Telecommunications, data centers, and climate change

Telecommunications and data centers are technologically advanced sectors of the US economy. They provide significant value as industries in their own right as well as services facilitating the communications and operations of the government and every data rich sector of the global economy reliant on advanced communications and digital technologies. The US telecommunications market is the largest in the world, with over 290 million wireless customers in the US, and continues to experience rapid growth and technological development (Verizon, 2011). With the advent of cloud computing and big data, data centers are increasingly relied upon as backbones of the information economy(Ricardo-AEA, 2014). These realities increase US reliance on telecommunications and data center sectors, making them, along with transportation, power, and water, critical components in the functioning of the US government and the global economy.

Due to their importance, disruptions to telecommunications and data center services companies produce ripple effects across their user base. Climate change (which can include both slow-onset, incremental changes as well as the increasing intensity and/or frequency of extreme events) can alter the baseline of expected conditions, causing impacts to companies in both sectors, their suppliers, and customers. The assets, equipment, and operating procedures of these sectors were designed to function within specific climate and environmental conditions. Impacts may result in changes to functionality, quality of service, return on investment, business continuity, and cost, in addition to cascading impacts to the diverse customers that rely upon them. The consequences of extreme weather events on these sectors is already beginning to be noted (Svenson, 2012; The World Bank, 2012).

Report objectives

The US General Services Administration (GSA) supports the functions, administration, and procurement of the Federal Government, and as such needs to understand and mitigate risks to vital services. Despite their importance, climate risks to the telecommunications and data centers services sectors remain insufficiently understood. The objective of this report is to better inform GSA's climate change adaptation planning and risk management activities by collecting, reviewing, and summarizing published information on climate risks in both sectors.

This report, prepared in accordance with the Climate Change Adaptation Action Plan (GSA, 2012), provides a foundational understanding of climate risks of both sectors, identifies gaps in existing knowledge, and makes recommendations for next steps.

Overall approach

A number of discrete tasks were undertaken in preparation for this report:

- Supply chain mapping
- Literature scan and gap analysis
- Annotated bibliography
- Recommendations

The methodologies and results for these are presented in the sections below. The concluding section with Recommendations synthesizes the results of the previous sections and suggests next steps.

2. Climate Risk in Telecommunication and Data Center Supply Chains

As facilitators and members of the global economy, the telecommunications and data centers sectors rely on networks of international supply chains. These supply chains offer customers sophisticated services as the result of coordination of inputs and services by suppliers. However, this complex network means that climate impacts to one part of the supply chain in one part of the world can have consequences for other parts of the supply chain in other parts of the world. A single climate event can have compound effects, with a range of direct and indirect impacts, across sectors.This was notably demonstrated in the 2011 Thai floods, as illustrated in **Figure 1**, when severe flooding disrupted electronics manufacturing in Thailand, leading to expensive delays and disruptions to companies around the world.

Understanding the range of climate risks facing the telecommunications and data centers sectors requires an understanding of the linkages between these and other sectors. In this section we present two complementary approaches for understanding the structure and interdependencies of these sectors, and discuss how to support identifying and assessing climate risk.

Supply chain maps

Supply chain maps visually depict the flow of goods and services that companies rely upon to operate. They provide a useful framework to assess climate risk in the telecommunications and data center sectors. Risks in one part of the world can affect other parts, just as impacts to one sector are rarely limited to that sector. Both telecommunications and data centers may experience climate impacts indirectly when the suppliers of key inputs and services on which they rely, such as electricity and parts manufacturing, experience climate impacts.

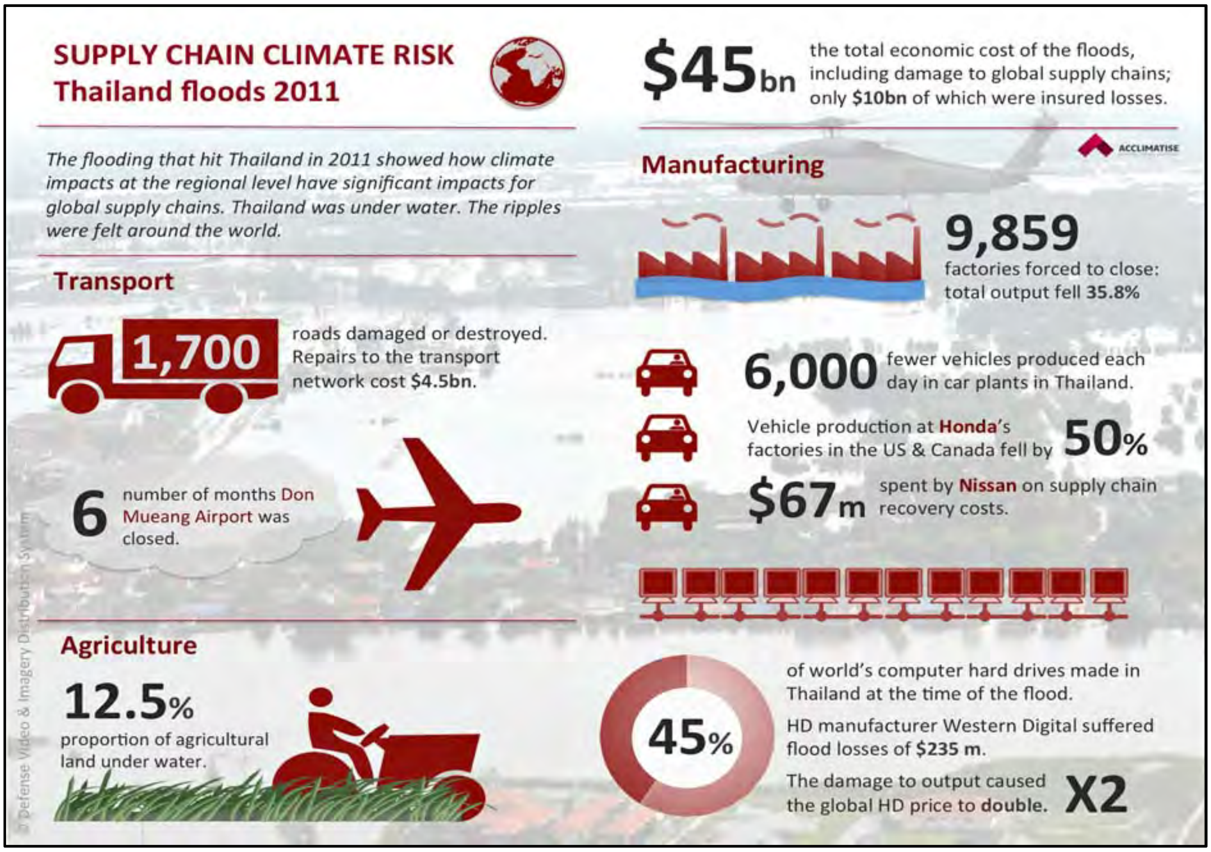

SUPPLY CHAIN CLIMATE RISK
Thailand floods 2011
The flooding that hit Thailand in 2011 showed how climate impacts at the regional level have significant impacts for global supply chains. Thailand was under water. The ripples were felt around the world.
Transport
1,700
roads damaged or destroyed. Repairs to the transport network cost $4.5bn.
6
number of months Don Mueang Airport was closed.
Agriculture
12.5%
proportion of agricultural land under water.
$45bn
the total economic cost of the floods, including damage to global supply chains; only $10bn of which were insured losses.
ACCLIMATISE
Manufacturing
9,859
factories forced to close: total output fell 35.8%
6,000
fewer vehicles produced each day in car plants in Thailand.
Vehicle production at Honda's factories in the US & Canada fell by
50%
$67m
spent by Nissan on supply chain recovery costs.
45%
of world's computer hard drives made in Thailand at the time of the flood.
HD manufacturer Western Digital suffered flood losses of $235 m.
The damage to output caused the global HD price to double.
X2
© Defense Video & Imagery Distribution System

Figure 1 - Supply chain climate risk: Thailand floods 2011 (prepared by Acclimatise 2012)

They may also be affected by changes in consumer needs and expectations in response to changing conditions. A further connection to resilience comes out of the importance of these sectors coordinating responses in periods of disaster. Strengthening the resilience of these sectors will improve the resilience of all the other sectors that rely upon them.

In this section, supply chain maps (seen in **Figures 2** and **3**) depict the essential constituents and relationships in both sectors. The objectives for this approach were to:

1. Include all the major elements of a typical supply chain for both sectors;
2. Present a generic sector supply chain that diverse companies in the sector can see the essential structure of their business within it;
3. Show and differentiate where and how climate impacts may present material risks or new opportunities across the supply chains; and
4. Stimulate and inform discussions on climate risk and opportunities within and between companies, suppliers, regulators, and customers.

The supply chain figures are each split into three parts to reflect three primary tiers:

- **The telecommunications/data center service provider**. This part of the supply chain contains core assets and operations which are vertically integrated and located within business fence-lines. Climate risks in this tier are generally more direct and can be addressed directly by the company;
- **Primary inputs**. These essential, horizontally integrated inputs are necessary for the successful functioning of the supply chain parts (beyond business fence-lines). Some of these inputs are international. Climate risks to both sectors pose indirect impacts on the service provider; and
- **The larger business and regulatory environment**. These factors indirectly influence all aspects of the supply chain, and climate risks.

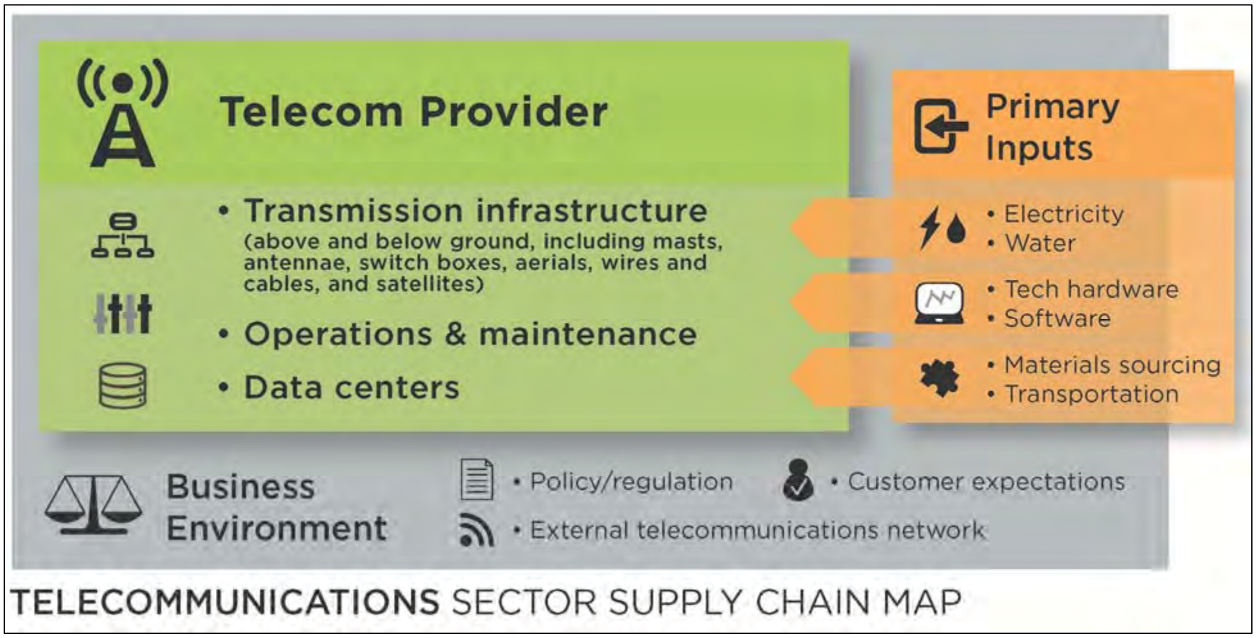

Telecom Provider
• Transmission infrastructure
(above and below ground, including masts, antennae, switch boxes, aerials, wires and cables, and satellites)
• Operations & maintenance
• Data centers
Primary Inputs
• Electricity
• Water
• Tech hardware
• Software
• Materials sourcing
• Transportation
Business Environment
• Policy/regulation
• Customer expectations
• External telecommunications network
TELECOMMUNICATIONS SECTOR SUPPLY CHAIN MAP

Figure 2 - Supply chain map for the telecommunications sector, demonstrating the chain of goods, services, and context that support and influence a company

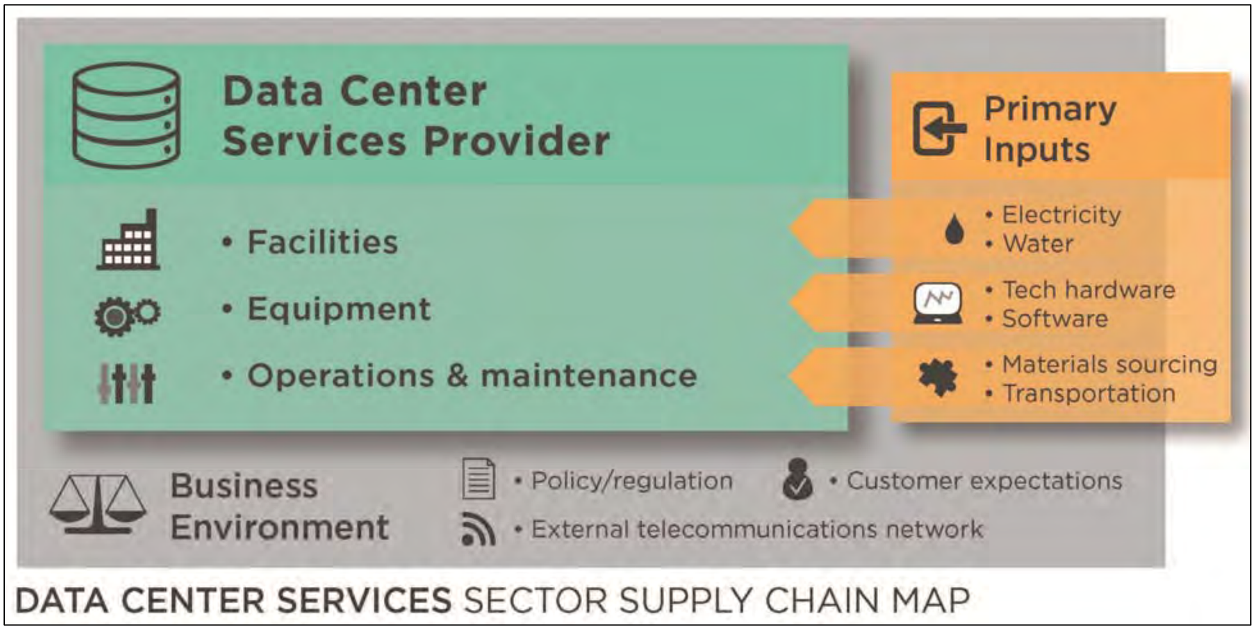


Figure 3 - Supply chain map of the data center services sector, demonstrating the chain of goods, services, and context that support and influence a company

The elements in each tier are organized according to the way the core service provider is influenced by them, as well as how that company can influence those elements. The level of influence a company has over different parts of its supply chain also affects the amount of information and influence a service provider has to understand and address climate risks in that part of its supply chain.

These supply chain figures are populated with a number of essential elements common to the supply chains of US companies in both sectors. Our team identified supply chain elements through a variety of methods, including through the sectoral definitions of the NAICS, the structure of representative companies, and the results of the literature scan. The value of material flows between sectors, and the interdependencies those indicate, can also be found in data from input/output use tables (see Annex 1). However, some key elements in both supply chains are not captured in input/output tables and yet may be influenced by a changing climate (such as government policy). These elements are also included in the supply chain maps.

Both the telecommunications and data center services sectors have a range of climate sensitivities, where the design and functionality of infrastructure, equipment, and operations can be affected by climate conditions. These include being sensitive to primary climate variables, such as average and extreme temperatures and humidity as well as secondary impacts such as flooding and landslides. These are examples of direct climate risks. Equally as important are the sensitivities to climate impacts outside the business fence-line, particularly access to a sustainable and resilient supply of inputs, such as energy and water, as well as the wider business operating environment that includes policy and regulation. These are sources of indirect climate risks. Though the distinction between direct and indirect risks is sometimes a blurred one – for example, impacts at the site will influence the requirement for energy, water, and supplies from outside – whether risks are direct or indirect affects the ability of a company to recognize and address these risks.

3. Literature Scan

This scan of existing publications on climate risk to telecommunications and data center supply chains provides a snapshot of the current state of global knowledge and experience in this area, identifies gaps and challenges, and lays a foundation for further analysis and recommendations. Those recommendations will constitute an early step toward building climate resilience in businesses in these two sectors, the US government, and all sectors that rely on telecommunications and data center services.

This literature scan reveals current knowledge on climate risks in both sectors. Our team found that this body of literature is small and limited, even when expanded to look at the broader information and communications technology (ICT) sector, which reflects that stakeholders in both sectors possess low awareness of climate risks. However, this scan identifies gaps and limitations in the current body of literature and presents complementary information, including case studies of climate impacts and adaptation responses, as well as highlights examples of synergies between adaptation and mitigation efforts in both industries.

All literature sources are captured in the References section at the end of the report. Those references that substantially address the topic are also catalogued in an Annotated Bibliography.

Methodology

This section describes the methodology used to review the global literature covering climate risk issues in the telecommunications and/or data center supply chains. It should be noted that these resources do not share a common terminology defining 'telecommunications' and 'data center services,' unlike the NAICS definition. In particular, much of the relevant literature on climate risk couches both sectors within the wider information and communication technologies (ICT) sector. For instance, only a few reports focus explicitly on telecommunications (ClimAID, 2011; Garnaut, 2008, Victoria, 2006), but many other reports on ICT provided relevant information.

Though the distinction between direct and indirect risks is sometimes a blurred one – for example, impacts at the site will influence the requirement for energy, water, and supplies from outside – whether risks are direct or indirect affects the ability of a company to recognize and address these risks.

To identify as many relevant insights from the literature as exist, our team used the NAICS sectoral definitions to identify references relevant to both sectors couched in broader discussions.

Our team looked to a broad range of potential sources of literature. To ensure the literature's relevance, our team prioritized domestic US sources, particularly resources made available by the US government and relevant trade bodies (including, for example, such organizations as the National Academies, National Telecommunications and Information Administration, United States Telecom Association, Telecommunications Industry Association, CTIA-The Wireless Association, Business Continuity Institute, Data Center Knowledge, and the US Department of Energy). Scanning for resources beyond the US, our team looked for literature from comparable countries and regions including Canada, United Kingdom (UK), European Union, Australia, and Japan, then searched more broadly across other international sources. Sources searched included government, environmental organizations, consultancies, academic publications, trade groups, and business associations. Scholarly sources were specifically sought out using academic online portals such as Science Direct and Google Scholar, as well as in the relevant climate literature (including, for example, reports from the Intergovernmental Panel on Climate Change and US Global Change Research Program (USGCRP).

A set of search terms was agreed upon intended to capture risks associated with climate change in both sectors, even if those risks were not explicitly associated with "climate." These terms included: climate change, adaptation, resilience, extreme weather, severe weather, heat wave, flood, storm, water, energy, and supply chain. A snowballing method, reviewing the references and works cited of useful documents, was employed to find additional resources.

Where specific telecommunications or data center companies were identified in the literature as having experienced climate impacts or taken adaptation action, the websites and annual reports of these companies were investigated for further details. Similarly, the results below demonstrate that there is significant interest in the UK on the topic of climate change in the ICT sector, leading to a more focused search for UK policy documents to identify adaptation strategies and principles.

Climate impacts

The ICT industry already experiences weather-related impacts, many of which are expected to increase in frequency and/or severity due to ongoing climate variability and climate change. Impacts, either observed or anticipated, are organized below according to climate variables. While some climate impacts present risks, there are others with potentially positive consequences that offer opportunities. The majority of this discussion focuses on telecommunications, of which much more literature is available than data centers, and is also a more heterogeneous sector, in terms of kinds of infrastructure and equipment widely used and thus exposed to a wider range of possible impacts.

In the literature, climate-related risks to the sectors are categorized in many ways, including by the following:

- type of climate hazard (Horrocks et al. 2010; ClimAID, 2011; ITU, 2014)
- business function/priority, (e.g. customer needs, product manufacturing and supply chain, workforce, infrastructure, business processes) (BSR, 2011)
- type of consequence (e.g. degradation of infrastructure, availability of services, quality of services, repair, cost, health and safety) (Horrocks et al., 2010)
- level of impact (e.g. national, local, individual/organizational (Horrocks et al., 2010)
- magnitude of climate change (e.g. extreme events and chronic change) (ITU, 2014)
- type of cost (e.g. operating or capital expenditures) (Garnaut, 2008)
- location of infrastructure (above or underground) (Horrocks et al., 2010)

The relevance of each categorization depends on the intended primary audience, for example, business (BSR, 2011), policymakers (Horrocks et al., 2010), or economists (Garnaut, 2008). The multitude of viewpoints illustrates the potentially wide reach of climate impacts. In this review, we have adopted a climate hazard framing, reflecting the vast majority of the literature reviewed, to illustrate potential impacts. These climate impacts are detailed for the telecommunications sector in **Table 1**.

Table 1 - Climate impacts associated with the telecommunications sector

Temperature

- Increases in temperature and higher frequency, duration, and intensity of heat waves create an additional burden on keeping equipment cool in exchanges and base stations, resulting in increased failure rates (Horrocks et al., 2010; ClimAID, 2011).
- Increases in mean temperature may increase the operating temperature of network equipment, leading to malfunction or premature failure if it surpasses design limits (Ofcom, 2010).
- Increases in temperature can stress telecommunications equipment and infrastructure, reducing life span (Horrocks et al., 2011; Garnaut, 2008).
- Increases in temperature may lead to an increase in heat-related health and safety risks to workers at telecommunications facilities, as well as at suppliers' sites (Horrocks et al., 2010; BSR, 2011).
- Increased energy demand during heat waves can result in power outages, which can affect the delivery of telecommunications services. Similarly, such disruptions can increase the cost of energy supply (BSR, 2011; ClimAID, 2011).
- Increased temperatures in winter may reduce cost of space heating in assets (e.g. exchanges), creating a cost-saving opportunity (Horrocks et al. 2010).
- Increased temperatures may reduce the frequency of the need to cope with snow-melt water surge (flood) problems in the long term, while in the short term, more rapid melt will increase flooding (Horrocks et al., 2010).

Precipitation

- Increased precipitation (rain or snow) leads to a higher risk of flooding low-lying and underground infrastructure and facilities, as well as erosion or flood damage to transport structures, potentially exposing cables (Horrocks et al., 2010; Ofcom, 2010).
- Icing during rain may impact telecommunication lines and infrastructure (ClimAID, 2011).
- Decreased precipitation can lead to land subsidence and heave, which can reduce the stability of telecommunications infrastructure both above and below ground (Horrocks et al., 2010; Garnaut, 2008; Ofcom, 2010).
- Decreased precipitation, in combination with increased temperatures, may increase the incidence of fires, which poses a risk to infrastructure, especially in rural or remote locations (Garnaut, 2008).
- Reduced snowfall may lessen the impact on transmission infrastructure, such as masts and antennae, requiring less upkeep or maintenance (Horrocks et al., 2010; Ofcom, 2010).
- Decreased precipitation may increase seasonal water scarcity, reducing the amount of water available for cooling (BSR, 2011).
- Increased precipitation and humidity can affect the radio spectrum on which wireless communications rely. Rain and snow absorb signals at some frequencies; therefore heavy precipitation can result in some transmitted signals not being received clearly or at all. Some services may also require increased transmission powers in order to withstand poorer weather without experiencing outage. As a result, this could limit the number of users supported in a given spectrum band (Ofcom, 2010).

Storms, wind, and extreme events

- Increases in storm frequency or intensity increase the risk of damage to above-ground transmission infrastructure (masts, antennae, switch boxes, aerials, overhead wires, and cables), which are often final access connections to homes and businesses, and may negatively impact telecommunications service delivery (Horrocks et al., 2010; Ofcom, 2010).
- An increase in storm frequency could lead to more lightning strikes, which can damage transmitters and overhead cables, causing power outages (Horrocks et al., 2010).
- Increased frequency and intensity of extreme weather events around the world increase the risk of interrupting materials supply (by disrupting air and sea transport) and manufacturing operations (Horrocks et al., 2010; BSR, 2011). For example, the 2011 Thai floods showed how climate impacts at the regional level can affect global supply chains (see Figure 1).
- Increased frequency and intensity of extreme weather events increase the risk of disruption to the electricity supply on which telecommunications rely (ClimAID, 2011).
- Extreme weather events may make it difficult for employees to get to work or for maintenance employees to access infrastructure, particularly in remote transmission networks (BSR, 2011; Ofcom, 2010).

Humidity

- Changes in humidity may lead to changes in patterns and rates of the corrosion of equipment (Horrocks et al. 2010).
- Higher levels of humidity may also lead to new dehumidification requirements to maintain internal environments within system tolerance ranges, as too much condensation can lead to short-circuiting or lead to water ingress (Horrocks et al. 2010).

Sea-level rise

- Rising sea levels and corresponding increases in storm surges increase the risk of saline corrosion of coastal telecommunications infrastructure as well as erosion or inundation of coastal and underground infrastructure (ClimAID, 2011).
- Sea-level rise may also lead to changes in the reference datum for some telecommunication transmission calculations (Horrocks et al., 2010).
- Rising sea levels will impact the operation of data centers and service centers upon which telecommunications rely (Horrocks et al., 2010)

There has been limited research to date into the impact climate change is having and may have on data centers specifically. However, as fixed installations with large energy and water requirements, data centers are likely to be vulnerable to the uncertain impacts of a changing and more variable climate, including many of the impacts listed above for telecoms. These assumptions (and more detailed research from other similar sectors such as energy and water) currently inform our understanding of climate risk at data centers.

It seems that they have a range of climate vulnerabilities, to both changes in average and extreme temperatures, as well as secondary impacts such as flooding and storms. These can be referred to as ‘direct climate risks.’ Equally as important are the sensitivities to climate impacts outside the data center fence-line; namely access to a sustainable and resilient supply of energy and water. These can be referred to ‘indirect climate risks.’ Often the distinction between direct and indirect risks is a blurred one – impacts at the site will influence the requirement for energy, water and supplies from outside.

Table 2 summarizes some of the direct and indirect climate risks that could affect the data center services sector and is based on a brief report issued by Acclimatise (2008).

Some further insights from the literature specific to data centers and climate impacts are discussed below.

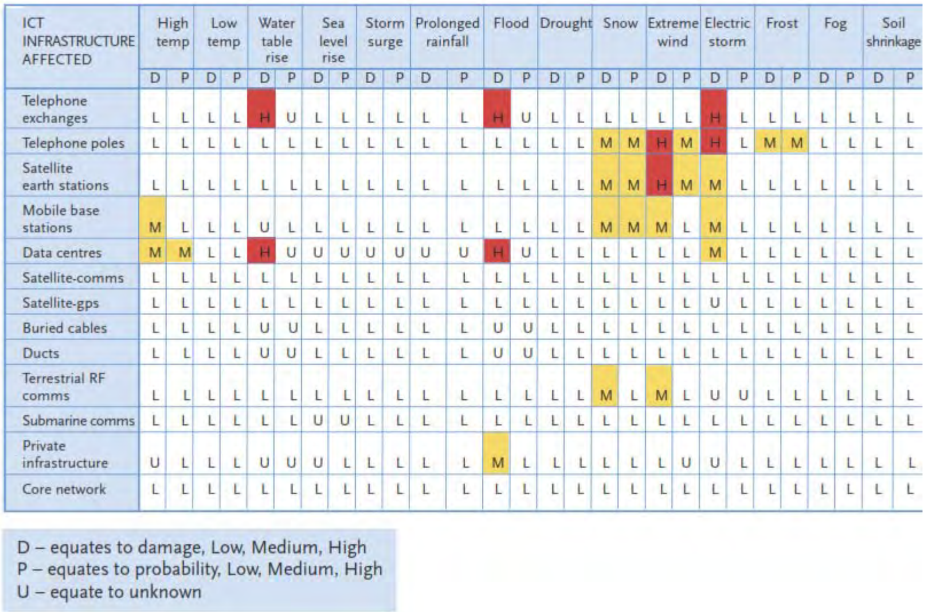
The most recent IPCC reports make reference to “a wide range of components and sub-systems for telecommunications systems that are within cities may need adaptation to the impacts of climate change – including telephone poles and exchanges, cables, mobile telephone masts and data centers.” (IPCC 5AR WGII, 2014). The research cited by the IPCC to justify this statement only briefly mentions data centers and presents an indication of which climate variables and impacts could pose an issue to data centers (see **Figure 4**) (Engineering the future, 2011). There is, however, no indication of how this matrix was constructed, and the approach is fairly generic and over-simplified. Nevertheless, it remains the only published example identified from the literature review of an attempt at developing a sectoral risk assessment exploring the probability and potential level of damage of a range of ICT assets to climate variables.

Despite this apparent lack of evidence, there is a sense amongst the business community that climate change could pose a significant threat to data centers and business operation in general. In a recent snapshot report of climate disclosures made by 270 of the largest European listed companies across 20 countries, the impact on data centers was brought up as a risk to business continuity. For example, the ING group was quoted as saying “(we) rely heavily on efficient data IT infrastructure to provide uninterrupted and efficient services to customers. In case of severe climate conditions leading to flooding (in our) data centers in the Netherlands, services to customers would be severely impacted.” (CDP, 2014)

Table 2 - Direct and indirect climate impacts associated with data centers (adapted from Acclimatise, 2008).[1]

Direct climate impacts
Additional burden on cooling equipment from increases in temperature and increased frequency of heat wave events
Reduction in operational efficiency and increased component failure rates as increases in average temperatures and associated humidity affect baseline design parameters. For example, the loss of ambient cooling potential.
Conflict between energy efficiency targets and short-term spikes or incremental increases in energy demand for cooling purposes
Increased demand for cooling during heat waves causing power failures in local transmission grids due to excessive loads.
Damage to operational equipment and potential loss of data through flooding of buildings, whether due to sea-level rise, increased river flood risk, groundwater or increased risk of ‘flash’ flooding when heavy precipitation overwhelms drainage systems
Damage to building fabric or overhead cables from storms; subsidence damage to underground communications infrastructure, with significant cost implications
Increased demand on backup power generators and batteries which have their own environmental impacts e.g. greenhouse gas emissions, hazardous waste.
Indirect climate impacts
Restricted supply of (cooling) water during periods of drought
Impacts on supply chains that provide replacement hardware
Workforce (both technical staff and security) affected by localized events and unable to travel to their workplace
Restrictions on energy supply due to heat waves and/or drought
Damage to upstream/downstream communications infrastructure e.g. by storms, flood or landslides.

[1] The climate risks listed in Table 2 are founded upon Acclimatise’s technical understanding of data centers’ equipment and operations in the context of existing expertise of climate risks to infrastructure and equipment generally.



ICT INFRASTRUCTURE AFFECTED	High temp		Low temp		Water table rise		Sea level rise		Storm surge		Prolonged rainfall		Flood		Drought		Snow		Extreme wind		Electric storm		Frost		Fog		Soil shrinkage	
	D	P	D	P	D	P	D	P	D	P	D	P	D	P	D	P	D	P	D	P	D	P	D	P	D	P	D	P
Telephone exchanges	L	L	L	L	H	U	L	L	L	L	L	L	H	U	L	L	L	L	L	L	H	L	L	L	L	L	L	L
Telephone poles	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	M	M	H	M	H	L	M	M	L	L	L	L
Satellite earth stations	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	M	M	H	M	M	L	L	L	L	L	L	L
Mobile base stations	M	L	L	L	U	L	L	L	L	L	L	L	L	L	L	L	M	M	M	L	M	L	L	L	L	L	L	L
Data centres	M	M	L	L	H	U	U	U	U	U	U	U	H	U	L	L	L	L	L	L	M	L	L	L	L	L	L	L
Satellite-comms	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L
Satellite-gps	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	U	L	L	L	L	L	L	L
Buried cables	L	L	L	L	U	U	L	L	L	L	L	L	U	U	L	L	L	L	L	L	L	L	L	L	L	L	L	L
Ducts	L	L	L	L	U	U	L	L	L	L	L	L	U	U	L	L	L	L	L	L	L	L	L	L	L	L	L	L
Terrestrial RF comms	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	M	L	M	L	U	U	L	L	L	L	L	L
Submarine comms	L	L	L	L	L	L	U	U	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L
Private infrastructure	U	L	L	L	U	U	U	L	L	L	L	L	M	L	L	L	L	L	L	U	U	L	L	L	L	L	L	L
Core network	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L

D – equates to damage, Low, Medium, High
P – equates to probability, Low, Medium, High
U – equate to unknown

Figure 4 - The low, medium, and high potential for different climate variables and impacts to have a negative impact on ICT infrastructure, including data centers (Engineering the future, 2011)

The reason for this apparent awareness of the threat of climate change comes in part from past experiences with extreme weather. While there is certainly a dearth of quantitative analysis with respect to data centers and climate risks, past events provide a tangible insight into the impact climate change is and will have on business continuity, not only for the data center owners and operators but also the customers who are increasingly reliant on their infrastructure and services (see **Table 3**).

Table 3 - Examples of weather event impacts on data centers in the US and UK

Rains flood Seattle T-Mobile data center (datacenterknowledge.com 4 Dec 2007)
The Seattle area was hit by more than four inches of torrential rain and gale-force winds, resulting in the flooding of a T-Mobile data center in Bothell, Washington. The flooding resulted in an outage that was reported to have taken down servers supporting the T-Mobile service activation portals and company websites. Account activations and the company website were affected, and no accounts could be accessed.

Hurricane Katrina damages data center (Computerworld 19 Dec 2007)
A data center serving 128 New Orleans public schools was located on the fourth floor of an administrative building when Hurricane Katrina hit. The hurricane blew the air conditioning system off the roof, allowing rain ingress. When power was restored, there was no air conditioning, and the rainwater and heat corroded contacts on switches. Other gear overheated and failed. Repairs to the data center cost in excess of $3 million and took several months.

Fasthosts knocked offline by stormy weather (ITproPortal 2014)
In January 2014 one of the UK’s largest internet hosting providers was knocked offline after stormy weather caused a power outage that left many customer without websites or email addresses. Compounding the issue what the fact that the firm’s communications systems were also affected which made it difficult to update customers during the disruption, which lasted several days.

Pipex-hosted sites impacted by flooding (The Register 27 Jun 2007)
Pipex was the first ISP to report major technical problems caused by extreme weather in the UK during summer 2007. A fiber break caused by flooding in the city of Sheffield affected two data centers located in two other cities, impacting the firm’s domain hosting business 123-reg. Customers experienced extended delays in communication between the north and south of England for approximately 1.5 hrs.

]

Discussion

There are several common themes in the literature on the character of climate risks to both telecommunications and data centers. A central theme revolves around the magnitude of impact and the rate of change associated with climate change. Furthermore, many of the features of both sectors create a complex relationship to climate change, influencing their vulnerability and providing both challenges and opportunities to adapt. Many of these factors also interrelate to each other; for example, shorter infrastructure lifespans and rapid technological change create an additional level of complexity. Likewise, there is an important interplay between water and energy. These elements are further explored below.

A. Short-term and long-term change

An important distinction raised is between the future impact of short-term extreme weather events and long-term incremental climate change. There is acknowledgement in the literature that changes in the nature and frequency of extreme events are currently of most concern, with less attention given to slow-onset changes (Horrocks et al., 2010; ITU, 2014). Extreme weather events dramatically show the potential economic cost of climate change in the near term, and some companies are already responding to these types of events. However, cumulative or gradual climate impacts are less likely to be on companies' radars due to associated uncertainty, failure to spot the signals, the absence of a driving motivation like an extreme event, and short-term business decision-making time frames. These impacts can lead to incremental costs and can decrease the expected lifespan of assets and infrastructure (IISD, 2013). Incremental changes also reduce operating margins and thresholds, which may not be immediately obvious in the short-term. The risk is that this also reduces the operating margins for handling extreme events.

B. Uncertainty of climate change

Some authors suggest that it is the currently unknown potential of future climate change impacts, expected to be characterized by low probability but high magnitude, which pose the greatest risks to the sectors. These potential risks include, from a UK source, fires from excessive heat beyond design standards or flood damage to critical system components (Baglee, Haworth, & Anastasi, 2012). In addition, there is more literature on the first-order impacts of extreme events and weather on telecommunications (Quanta Technology, 2009), and relatively little evidence of assessments on secondary or tertiary climate change impacts. Similarly, there is more emphasis on climate risks to infrastructure than to the enterprise supply chains that support business in both sectors. Though literature on climate risks in both sectors is scant, more of what is available focuses on telecommunications.

Extreme weather events dramatically show the potential economic cost of climate change in the near term, and some companies are already responding to these types of events. … These impacts can lead to incremental costs and can decrease the expected lifespan of assets and infrastructure. Incremental changes also reduce operating margins and thresholds, which may not be immediately obvious in the short-term. The risk is that this also reduces the operating margins for handling extreme events.

C. Business timescales

First, telecommunications infrastructure lifespans are typically shorter than those of other infrastructure types (for example, energy, water, or transport) and are thus not as great a liability (Horrocks et al., 2010). Much of the infrastructure in use today in the UK for example, apart from towers, cables, and underground tunnels, will be replaced before the 2050s (ibid.). In addition, the pace of technological development is rapid. These factors combined present both a challenge and an opportunity.

On the positive side, rapid technological development and shorter infrastructure lifespans provide inherent flexibility and ability to respond quickly to changes in climate, providing an existing level of resilience (ibid.). However, this also means that the sector does not take a very long-term view of planning. This is compounded by the high level of competition within the sector. The US telecommunications industry is almost entirely privately owned and highly competitive, in contrast to other service industries that rely on large infrastructure (ClimAID, 2011). This means there can be a tendency to focus on profitability and short-term market share rather than on adopting longer-term strategies that take into account future climate change. Longer-term strategies might involve improving the resiliency of infrastructure rather than simply replacing it as it is damaged (ibid.).

D. Interdependencies

Virtually every sector is dependent on telecommunications. Emissions mitigation policies in other industries often encourage telecommuting through remote working or teleconferencing in place of travel. Thus mitigation efforts across other sectors will depend on the ability of telecommunications (and more broadly, ICT), to adapt (Horrocks et al., 2010). In addition, the consequences of future impacts of climate change will be greater, as reliance on telecommunications will only increase (Baglee et al., 2012). There is a significant need to map out the relationships between telecommunications and other sectors.

The telecommunications sector is also characterized by interdependency within its own network, as well as among other sectors, notably water, energy, and transport (Defra, 2011; URS, 2010). Data centers are highly interdependent on energy and water. Interdependencies compound the impacts that can be felt in the wake of extreme events. For instance, when there was a loss of power during Hurricane Sandy, users had trouble finding energy to charge cell phones and the backup batteries in cell towers were quickly exhausted (Kahn, 2012).

Another type of interdependency relates to shared infrastructure, which is increasingly a feature of the telecommunications industry in the US and internationally. To achieve economies of scale, in response to both regulation and commercial interest, companies adopt a variety of infrastructure sharing models, sharing both passive (non-electronic, such as towers, base trans-receiver station (BTS) shelters, and power) and active (electronic, including spectrum, switches, and antennae) infrastructure. While this contributes to business efficiency and encourages new entrants to the market, it may have a negative impact on the resilience of the telecommunications system by increasing the dependence of one party on another, not all of which may meet the same standards of resilience. Likewise, shared infrastructure reduces redundancy across the entire domestic network. Thus, the “ability to operate locally becomes dependent on artifacts of the system which will be remote from the user, under the control (operational and legal) of other parties and generate potential single points of failure” (Horrocks et al., 2010). Furthermore, because telecommunications companies do not own the entire infrastructure they use, like cell towers, there is less incentive to invest in building climate resiliency.

E. Equity

A recurring question in the literature is how equity is affected depending on whose resilience is being considered. While from a national perspective, telecommunications systems may already be resilient for the reasons cited above, from an individual end-user perspective (household or business), what matters is the availability and quality of services from their local telecommunications network (Horrocks et al., 2010). Different parts of society, such as low-income, elderly, sick, or rural groups, are more exposed than others to climate risks in the telecommunications sector. In addition, it may be difficult for people in those groups to report outages during extreme events and emergencies, such as during ice and snow storms when mobility is limited (ClimAID, 2011). The issues surrounding equity with respect to remote access hold particular importance in the US due to its geographical expanse. Compounding this is the fact that there is less understanding of the specific impacts of climate change impacts on local communities.

There are also equity considerations in the corporate world, particularly in terms of small- and medium-sized enterprises relative to large corporations. The latter, often based in urban areas, have flexibility in managing their telecommunications systems and are able to transfer ICT requirements among sites around the world to avoid risks, while the former are more likely to have single sites and less capacity to plan or invest in future resilience, and are thus more vulnerable to weather-related disruptions (Horrocks et al., 2010). This is an important point considering the small business procurement goals US federal agencies are required to meet. Similarly, there are higher risks to employees who work remotely and rely heavily on telecommunications.

F. Water

The enormous volume of water required to cool high-server-density centers is making water management a growing priority for data center operators. This importance has encouraged data center operators to upgrade local water resources infrastructure, often with co-benefits for the local community. For example, in a move that will reportedly "save millions of gallons of potable water for the local community," Microsoft has teamed up with the City of Quincy, Washington to retool the city's water treatment infrastructure. As part of the partnership, a multi-million dollar drinking-water treatment plant built by Microsoft to support its data center will be leased to the City of Quincy for just $10 a year. The plant will be retrofitted and expanded to support the water reuse initiative, which will allow other nearby businesses and data centers to benefit (Miller, 2013). Elsewhere in northern Europe, Google has recently implemented a cooling system which uses sea water at one site at Hamina, southern Finland (Google, 2014).

The National Security Agency (NSA) provides a further example of data center operators taking action to improve water supply security. A new data center being built by the agency will use up to five million gallons a day of treated wastewater from a Maryland utility. The agency recently reached an agreement with Howard County to use treated waste water – also known as "grey water" – that would otherwise be discharged untreated into the Little Patuxent River (Miller, 2013).

The reports from Microsoft, Google, and the NSA do not, however, make any suggestion that the upgraded drinking water treatment and waste water treatment facilities will be designed to be resilient to changing climatic conditions, such as changes in seasonal precipitation regimes.

There have also been examples of alternatives to the use of large volumes of water for cooling data centers. We are beginning to see data centers using dry coolers (closed loops) to cool data centers in combination with operating equipment capable of operating at higher temperatures based upon revised guidelines (e.g. DOE, 2014b). This is part of a trend toward increased acceptance for less stringent guidelines with respect to cooling hardware. For example, best practices are making their way into the market thanks to organizations such as the American Society of Heating and Air-Conditioning Engineer's (ASHRAE) published guidelines for classes of computer servers showing that the equipment can operate at higher temperatures. The Green Grid also published guidelines and maps showing that free cooling[2] is possible for a significant portion of the year across most of the US. However, these changes do not take into account that as ambient air temperatures increase it may mean the opportunity to operate equipment without cooling diminishes. This could also mean the new guidelines would be quickly outdated. A more durable approach would be to understand the temperature range and the efficiency fall off that servers can operate within. This then mapped against increasing temperatures would give you an optimum point at which you need to switch to a cooling system.

G. Energy for data centers

The importance and recognition of addressing energy consumption is spreading in the data center sector. The US Department of Energy's Federal Energy Management Program highlighted the need for data center owners to "employ industry energy efficiency best practices to lower both capital and operating costs, while ensuring sustainability through reduced energy and water use" (Tschundi, 2013). In the UK, data centers typically see turnover growth rates of 15 percent per year. In the face of growing energy demand (and associated costs), the UK government has recently announced the intention to extend Climate Change Agreements (CCAs) to the data center industry, which will provide incentives for the industry to become more energy efficient (Ricardo-AEA, 2014). In both cases, there was, however, no indication that climate change impacts should be taken

[2] 'Free cooling' is the method of employing relatively colder external air temperatures to cool internal systems without the use of air conditioning.

into consideration explicitly in this decision-making process.

There has been a recent trend to locate data centers in cooler climates in remote locations. For example, Facebook recently revealed plans to locate one in Lulea, Sweden, right on the edge of the Arctic Circle (Stevenson, 2014). The aim is to reduce the need for active cooling, therefore reducing energy costs. A reported co-benefit is that the local community benefits from the heat generated by the servers during the winter months. The reduction in the amount of cooling required does not necessarily protect the site from other impacts, like storms or permafrost melt. For the US Government and many US-based companies, however, location sites are for security reasons limited to domestic regions.

Recent reports suggest large data center operators, such as Apple, are investing in their own renewable energy in order to deal with the growing need for energy (Sverdlik Y., 2014). While this has clear implications for climate change mitigation, it was not suggested in the reports that future climate conditions were taken into consideration when designing and installing the energy generation infrastructure.

Lawrence Berkeley National Laboratory (LBNL) evaluated three data centers for potential energy efficiency improvements during the summer of 2012. It was concluded that annual cost savings can be achieved by simply aligning IT rack units and equipment rows into hot and cold aisles (Mahdavi, 2014). Relatively straightforward modifications to center configurations can form the basis of climate risk management measures (see **Table 4**). In this instance, LBNL highlighted a potential way data centers could be designed or upgraded to ensure they are equipped to provide the cooling needed to ensure processors, servers and other equipment can operate efficiently and prevent servers failing in the face of increasing temperatures and humidity.

There have been suggestions that on-site combined heat and power (CHP) technologies could improve energy reliability and reduce costs at data centers (Darrow, K. and Hedman, B., 2009; Miller, 2014 A). It is argued that a broader application of CHP will lower demand for electricity from central stations and reduce the pressure on electric transmission and distribution infrastructure. While extolling the virtues of such technologies, there has been little discussion about the possible impact of climate change on the efficiency and reliability of this form of energy generation. For example, power generation of a Combined Cycle Gas Turbine (CCGT) facility varies with ambient temperature, which affects the net power generated in the gas and steam cycle (Arrieta and Lora, 2005).

Data center operators are also using the availability of local, cheap hydropower as a way of reducing energy costs. For example, the operator ROOT has recently lowered collocation prices in Montreal because of the “cheap hydro power, cool climate and great connectivity to New York, Toronto and Europe” (Verge, 2014). Again, however, there is no attention paid to the potential longer-term impact of climate change on the availability and reliability of this hydropower as hydrological systems are perturbed.

H. Energy for telecommunications

There is similar recognition in the literature of the telecommunications sector’s reliance on energy. Cooling and operating information and telecommunications technology equipment accounts for 1.5 percent of the energy consumption in the United States and is growing (The Economist, 2008, in ClimAID, 2011). This reliance increases the sector’s vulnerability to climate variability and change, as disturbances to the power grid often affect telecommunications infrastructure (ClimAID, 2011). For example, in the US, telecommunications and power lines often share the same poles (ibid.). However, there has been little detailed assessment of how climate change impacts the link between energy and telecommunications, despite the recognition that this is a “critical dependency” (Horrocks et al., 2010).

Climate impacts on power supply include extreme weather, such as ice and snowstorms, thunderstorms, and hurricanes, also pose a risk to telecommunications because they may damage infrastructure. A 2006 snowstorm in western New York helps illustrate this vulnerability. An early wet snow caused tree branches to break and damage power lines, causing 93,000 reported disruptions to telephone service in about 30 days (ClimAID, 2011). Gradual changes in climate are also important, as increased temperatures and heat waves may lead to brown- or blackouts from overload due to increased demand for electricity for air conditioning (ClimAID, 2011).

The reliance of the telecommunications sector on the electricity grid means that vulnerability is exacerbated in remote areas that are not well connected to the grid. This has prompted some companies to use renewable energy solutions to power telecommunications infrastructure. For example, Verizon employs a hybrid renewable energy microgrid to power its telecommunications tower in a remote ski site in Northern California (Marketwired, 2014).

There is also a question in the literature about the increased need for energy in new generation technologies, which are faster and require more processing capacity, despite generally being more energy efficient. Whether or not the increased energy demand will cancel out the benefits of energy efficiency is a question for further research (ClimAID, 2011).

An adaptation strategy includes the implementation of procurement processes (both corporate and government) that require an improved level of climate resilience, emphasizing service continuity rather than compensation for disruption. This would help create a market for climate resilient services and encourage telecommunications service providers to incorporate additional climate resilience into their prices.

I. Adaptation strategies and principles

This section describes the range of adaptation strategies and actions identified in the literature that telecommunications and data center companies are taking in response to extreme weather or climate change. These come both in the form of recommendations of future actions as well as in observed practice. Adaptation initiatives are categorized within the following broad strategic categories: technical, strategic, and institutional. Where possible, examples are used to illustrate these strategies and actions.

J. Technical

Throughout the literature, most adaptation actions underway or recommended are technical fixes or adjustments. These options generally involve engineered, built environment, and technological solutions; the improvement of existing practices and the development of new ones; as well as improved planning, maintenance, and design. These types of actions relate to the following business activities, categorized by BSR (2011) as “value protection” strategies: site and asset risk assessments and continuity planning; strengthened resilience of business assets and processes; improved resource efficiency and conservation in manufacturing sites and processes; supply chain risk assessment and management; and workforce protection. It should be noted that within these categories, the current focus of the literature is on adaptation options pertaining to physical sites, assets and processes, and less on supply chain activities and relationships which are further removed from the business itself. **Table 4** describes these actions in detail.

Table 4 – Adaptation actions focused on physical sites, assets, and processes from the literature

Strengthened resilience of business assets and processes

- Use reprogrammable or “chameleon” technologies, which can enable a range of different functions, each configured for the particular environmental conditions encountered during a product’s life (Horrocks et al., 2010).
- Make the core/backbone, the transmission line that carries data gathered from the smaller lines with which it connects, redundant for all service areas and resilient to all types of extreme weather events; provide reliable backup power with sufficient fuel supply for extended grid power outages (ClimAID, 2011).
- To reduce vulnerability of flooding in central offices, raise equipment from the ground floor to higher floors. This has already occurred many times when obsolete electromechanical switches were replaced by smaller digital switches, causing complete floors to be vacated.
- Develop a set of minimum national standards for telecommunications infrastructure resilience, potentially in line with ‘commercial decision’ standards, to 1) identify potential weaknesses and 2) stimulate adaptation action (Horrocks et al., 2010).
- Introduce strategic or dynamic nodes for specific locations to enable interconnectivity under disaster conditions, particularly in rural areas (Horrocks et al., 2010).
- Decouple communication infrastructure from electric grid infrastructure to the extent possible and make more robust, resilient, and redundant (ClimAID, 2011). This could, for example, involve the use of microgrids. Urban Green Energy (UGE), a distributed renewable energy solutions provider, has a particular service offering for telecommunications companies to ensure constant uptime. The company was recently contracted by a confidential Middle Eastern government entity to provide distributed renewable energy microgrids to power its remote telecommunications towers (Marketwired, 2014).UGE has also provided hybrid renewable energy solutions to a telecommunications tower operated by Verizon in a remote ski site in Northern California. These types of solutions, typically used for telecommunications needs in emerging markets and remote locations, may also prove useful in strengthening climate resilience more broadly, in urban centers as well as hard-to-reach places.
- Implement procurement processes (both corporate and government) that require an improved level of climate resilience, emphasizing service continuity rather than compensation for disruption. This would help create a market for climate resilient services and encourage telecommunications service providers to incorporate additional climate resilience into their prices. Although there is little evidence of procurement processes and specifications being changed to take into account the impacts of a changing climate, this is seen by this report's authors as a critical adaptation action. There may also be a need for a government role to coordinate services provided to ensure national interests, as well as commercial needs are represented (Horrocks et al., 2010).
- Minimize the effects of power outages on telecommunications services by providing backup power at cell towers, such as generators, solar-powered battery banks, and “cells on wheels,” or COWs, that can replace disabled towers. Extend the fuel storage capacity needed to run backup generators for longer times (ITU, 2014).
- As stresses on the grid system increase with rising temperatures, data center operators must ensure uninterruptable power supplies are maintained and tested regularly and that backup generators have adequate fuel reserves on-site. Proper maintenance of generators is also important, for example they need weekly testing/cycling (Acclimatise, 2008).
- Protect against outages by trimming trees near power and communication lines, maintaining backup supplies of poles and wires to be able to expediently replace those that are damaged, and having emergency restoration crews at the ready ahead of the storm’s arrival (ITU, 2014).
- Increase resilience against temperature increases could involve developing computer chips which will operate at higher optimal temperatures (Horrocks et al, 2010).
- Relocate central offices that house telecommunications infrastructure, critical infrastructure in remote terminals, cell towers, etc., and power facilities out of future floodplains, including in coastal areas increasingly threatened by sea-level rise combined with storm surges (ITU, 2014).

- Place telecommunication cables underground where technically and economically feasible (ITU, 2014), and design them to withstand hotter temperatures and an increased risk of groundwater flooding and subsidence, possibly exacerbated by increased temperatures and reduced summer rainfall (Defra, 2011).
- Replace segments of the wired network most susceptible to weather (e.g., customer drop wires, which extend an open wire from a pole to a building) with low-power wireless solutions (ITU, 2014).
- Data center operators should consider establishing the ability to switch the computational load to other data centers in their networks in cooler locations around the globe (Horrocks et al., 2010).
- Develop high-speed broadband and wireless services in low-density rural areas to increase redundancy and diversity in vulnerable remote regions (ITU, 2014).

Improve resource efficiency and conservation in manufacturing sites and processes

- Minimize consumption of and reuse resources in response to increased demand and decreased availability and reliability of supply (BSR, 2011).
- Implement energy-efficiency initiatives
- Assess and implement renewable energy initiatives

Supply chain risk assessment and management

- Evaluate supply chain risk due to climate change and develop business continuity plans (BSR, 2011). An example from the wider ICT sector is that of EMC, whose Global Supply Chain group’s business continuity program assesses the potential impact of events on its suppliers and ensures that mitigation plans are in place for all medium- and high-risk areas and suppliers, a process that could integrate climate risk management into existing supply chain management (ibid.).
- Assess disaster recovery processes and to what extent they take account of possible extreme climate events which may disrupt the distribution of new equipment. A key focus could be on potential transport problems caused by climate-related disasters (ITU, 2014).

Site and asset risk assessments and continuity planning

- Improve the spatial planning of the location of key buildings and facilities, taking into account climate change considerations. When assessing international locations, operators and owners should assess the risks associated with changing climate hazards in each country. Decisions made today based on historic operating and maintenance costs for a country may not be robust in the face of inevitable climate change and may impact financial viability. For example, natural hazards exposure maps specifically for US-based data centers have been developed (Uptime Institute, 2010). Another example is from Telecom NZ, a New Zealand telecommunications operator, which reports that it is actively involved in mitigating flood risk by reviewing design standards and facility location, though no further details are publicly available (Telecom NZ, 2014).
- Assess the location of backup generators, which are often located outside the main building near ground level, and raise them if necessary to reduce the risk of failure due to flooding. Flood maps may be used for this exercise, available online from the Federal Emergency Management Agency (FEMA) (ITU, 2014) – see https://msc.fema.gov/portal
- Incorporate climate change into existing corporate risk assessment procedures, enterprise risk management (ERM) systems, and business continuity programs. For example, climate risks form part of the operational risks in Telefonica’s risk management model (ITU, 2014).

Workforce protection

- Monitor and protect workforces against potential health risks (BSR, 2011).
- Explore opportunities for remote working (ITU, 2014).
- Understand where workers live and how their journey to work will be affected by an extreme event, noting that even if the sectoral assets are resilient, the workers needed to operate them may not be able to get to the site, either because of access and transport disruptions or because they are faced with personal challenges (e.g. homes are flooded).

K. Institutional

Institutional options involve the design and amendment of laws and regulations, the design and implementation of government policies and programs, and financial/economic options that incentivize building resilience.

UK policy provides an example of adaptation strategy at the national government level. The UK Climate Change Act of 2008 gives the Department of Environment, Food and Rural Affairs (DEFRA) Adaptation Reporting Power the authority to request that the organizations responsible for essential services and infrastructure (including telecommunications regulator Ofcom) report on the current and future predicted risks and impacts of climate change on their organization and their proposals for adapting. These requests have been found to be important in providing a framework for greater consideration of climate change by key infrastructure organizations, in building capacity to assess and monitor climate risks, and in providing examples of best practice (Cranfield University, 2012, in IIED, 2013). However, it should be noted that Ofcom has limited statutory duties in relation to resilience and its regulation (Horrocks et al., 2010). Ofcom itself states in its report that it is unable to provide a detailed assessment of climate impacts on the sector, because this type of data is held by operators and will differ based on the specific network, physical location, and planning rules (Ofcom, 2010). Therefore, engagement of telecommunications service providers in providing a more complete picture of climate vulnerability and risk is crucial (UKCIP, 2013).

The UK government also carried out an Infrastructure and Adaptation Project that examined the risks to four infrastructure sectors (including ICT) and identified potential solutions for improving climate resilience of new and existing infrastructure. This involved the commission and publication of four studies, one for each sector. The study relating to the ICT sector, “Adapting the ICT Sector to the Impacts of Climate Change” by Horrocks et al., stands out among the global literature on ICT and climate risk and is one of the primary sources used in the present report. These studies informed the 2011 update of the National Infrastructure Plan, as well as subsequent updates. Further research driven by government could be a way to increase consideration of climate change in existing and new infrastructure planning and identify priority action areas.

Another adaptation strategy is to reassess and develop industry performance standards to incorporate climate change considerations (ITU, 2014). The International Telecommunication Union (ITU), the specialized agency of the United Nations responsible for ICTs, has taken the lead on engaging the global community to address climate change through the use of ICTs. The Study Groups of ITU’s Telecommunication Standardization Sector (ITU-T) bring together international experts to develop international standards known as “ITU-T Recommendations,” which act as defining elements in the global infrastructure of ICTs. One of these groups, Study Group 5 – SG5, focuses on environment and climate change and includes a specific question on ICTs and adaptation. Specific work items for SG5 include (ITU, 2014):

- Recommendations to support adaptation to climate change and improve the resilience of the ICT infrastructure to the impacts of climate change
- Practical examples and best practices of ICT standards to support adaptation to climate change for countries and ICT sector.

The development of new standards for ICT and adaptation, which will encompass the telecommunications sector, would provide a common starting point to identify and reduce the risks due to climate variability and change.

L. Social

Social options involve educational, informational, and behavioral approaches to address climate challenges. The fact that little has been written about climate change risks in the telecommunications and data center sectors points to the lack of knowledge and awareness about potential climate change impacts on the sector. In response, research has been recommended as an adaptation strategy, both to better understand climate impacts on the sector and also to develop new technologies to respond to those impacts. Research and data collection recommendations include hazard and vulnerability mapping, a review of past weather impacts on telecommunications, risk assessments, and an assessment of the role of various stakeholders in addressing climate risks (Horrocks et al., 2010). In terms of innovation, areas for research and development include (ITU, 2014):

- Creation of a standardized charging interface so that any phone can be recharged by any charger
- Winning support for and developing alternative telecommunication technologies to increase redundancy and/or reliability, including free-space optics (which transmit data with light rather than physical connections), power line communications (which transmit data over electric power lines), satellite phones, and ham radio. (It should be noted that this adaptation of deploying power line communications conflicts with another adaptation strategy mentioned above: decoupling telecommunications infrastructure from the electric grid. This conflict illustrates the need for further research and cost benefit analysis of adaptation options.)

Awareness raising, among both telecommunications providers and their customers, is another recommended resilience-building strategy. One example is a telecommunications company educating users to not overload networks during a disaster by encouraging “customers to send a text message about the tornado, as opposed to taking a picture and sending it from their cell phone (which uses more network capacity)” (ClimAID, 2011). Another way to raise awareness is via platforms for dialogue and engagement. The UK Environment Agency’s Climate Ready Service has set up an Infrastructure Operators Adaptation Forum, which is composed of the country’s main infrastructure organizations, their regulators, and government departments. This provides a platform for these stakeholders to engage in discussion leading to a shared understanding of best practice in climate resilience (UKCIP, 2013).

M. Strategies at the adaptation-mitigation nexus

The telecommunications sector is highly dependent on the energy sector, and as such, contributes to GHG emissions (though its emissions are relatively small compared with other industries). Global telecommunications systems are estimated to account for about 0.7 percent of global CO2 emissions (Kelly & Adolph, 2008). However, due to the proliferation of telecom devices, as well as the need for more processing power for the growing transmission capacity of new generation technologies, emissions are predicted to increase more than twofold (ibid.). Cooling and operating information and telecommunications technology equipment already accounts for 1.5 percent of the energy consumption in the United States and is growing (The Economist, 2008, in ClimAID, 2011). It is thus important to consider mitigation in concert with adaptation. Adaptation strategies should not be implemented at the expense of mitigation, or vice versa, but optimal strategies would deliver progress against both goals.

Many telecommunications service providers both in the US and internationally engage in energy efficiency and renewable energy initiatives that provide benefits for building climate resilience as well as reducing GHG emissions. For example, in 2013, Verizon announced an investment of $100 million in a solar and fuel cell energy project which is expected to produce more than 89M kWh of electricity in its first year. That energy will power critical data centers, central offices, and buildings across six states. This will also eliminate more than 10,000 metric tons of CO2, which is enough to offset the annual CO2 emissions from more than 1 million gallons of gas (Verizon, 2013). This type of initiative is also adaptive as it reduces dependency on the electricity grid, which is expected to suffer as a result of increased energy demand during heat waves. The reduction will lessen the impact from power outages on the operator, which affect the delivery of services. This also reduces energy costs, savings that could be directed toward building resilience.

Energy efficiency initiatives often offer a number of synergistic benefits, such as cost savings, and most telecommunications companies engage in such initiatives for multiple reasons. Tata Teleservices, one of India’s main telecommunications providers, engages in energy efficiency initiatives, and while these are primarily aimed at reducing emissions, they also double as promoting adaptation. For example, the company has upgraded to heat-resilient equipment in its BTS stations, reducing the need for air-conditioning (and energy consumption) but also increasing resilience to rising temperatures (S. Mathew 2013 pers. comm, 8 August). Finally, with the increased mainstreaming of mitigation initiatives, this may provide an accessible avenue for also implementing resilience-building measures.

As demand for telecommunications services grows and as newer, faster technologies that require more capacity are introduced, it will be important to conduct research to evaluate the efficiency gains of new technology relative to increased energy use (ClimAID, 2011). Although new generation technologies tend to be more energy efficient, they require more processing power due to their higher transmission capacity and overall demand for these services keeps increasing, suggesting that total demand for energy may increase at faster rates than gains in efficiency.

While not necessarily focused on climate change, there is a growing body of research that examines how power, cooling, monitoring, and service inadequacies, particularly in the data centers sector, can contribute to a facility's risk of downtime and associated costs. That same body of research provides guidance for improved efficiency and resilience (Emerson Network Power, 2011; EPA, 2007; Brill, K.G. and Stanley, J., 2009). Indeed, in order to maintain 'up time' and reduce energy and water costs, there has been a great deal of focus on improving efficiency and reducing demand at data centers. Some of these efforts are likely to have the co-benefit of reducing carbon emissions and improving resilience to climate change. Recently, the DOE (2014a) has prepared a report -- The Water-Energy Nexus: Challenges and Opportunities – which could be relevant to data center developers and operators. The following section summarizes key case studies and developments in the industry.

Selected case studies

Early examples of the impacts of extreme weather or climate change on telecommunications demonstrate ways how companies can manage the technical, financial, and political challenges of addressing climate risk. Below are three case studies identified in the literature.

Verizon and Hurricane Sandy

Hurricane Sandy illustrated the impact of extreme events on the telecommunications sector. Several Verizon central offices in Lower Manhattan, Queens, and Long Island experienced flooding as a result of storm surge, which led to power failures and rendered the back-up power systems at these sites inoperable. According to federal regulators, Sandy knocked out about 25 percent of cell towers belonging to all carriers in a coastal area spread over parts of 10 states (Svensson, 2012). Cell towers often have battery backups in case of power outages, which provide power for various but short periods of time. Some towers also have backup diesel generators in case of battery failure. During the hurricane, telecommunication providers had to deploy these back-up generators and install new batteries at cell sites. However, as flooding makes cell towers unreachable, operators had to form makeshift cell towers, known as COWs, and cells-on-light-trucks or COLTs (Goldman, 2012).

The storm seriously impacted telecommunications service provision. AT&T released a statement warning that customers served by these central offices would experience a loss of all services including fiber-optic network (voice, Internet, and video), high-speed Internet, and telephone (ITU, 2014). However, the incident also prompted creative solutions. AT&T and T-Mobile USA joined together in an unprecedented arrangement, allowing their customers to roam for free on both networks to compensate for any gaps in coverage due to blacked-out cell towers (Svensson, 2012). In terms of financial impact, Verizon estimated that Hurricane Sandy cost the company about $1 billion.

Since Sandy, Verizon has implemented resilience-building measures, first of all replacing its entire copper wire network in Lower Manhattan with fiber-optic cables, which transmit data by a series of light pulses and are waterproof. Its vital underground fuel pump, which is meant to deliver diesel fuel to back-up generators, which stopped working due to flooding during the storm, is now protected in a watertight room with a submarine door (PBS Newshour 2013).

BT Group

BT Group is a widely cited example of a telecommunications company that has both felt the impact of climate change as well as undertaken adaptation initiatives in response. BT's Chief Sustainability Officer, Niall Dunne, expressed that "climate change is literally washing through our network," in reference to the problems the company has experienced from flooding at exchanges. In 2010, a major flood occurred at a BT exchange in Paddington, London, which led to an electrical fire and ripple effects at exchanges around the UK, affecting broadband and telephone services for several hours. Four hundred and thirty seven exchanges and up to 37,500 datastream circuits were affected (Baglee et al., 2012). The extent of the impact illustrates the interconnectivity of the telecommunications sector and how this interconnectivity can amplify the impacts across the sector. BT has since invested in making its underground network more resilient to flooding, laying cables that can better withstand water damage, for example switching from copper to fiber-optic cables. According to BT, this reduces network faults and improves the reliability of networks while cutting repair costs (BSR, 2011). BT is also now building and upgrading infrastructure based on likely flooding scenarios 50 to 100 years in the future. Though not a corporate social responsibility (CSR) initiative, this pragmatic action would, if neglected, result in a "customer service nightmare" (Acclimatise, 2013). Dunne also commented on the importance of the BT network as a strategic national asset and pointed to the importance of protecting it for the benefit of government and other critical users (Reuters, 2013).

Resilience-building Activities of US Wireless Providers

US telecommunications companies are already undertaking initiatives to build resilience in the face of extreme weather events, as illustrated by the example of the wireless industry. In 2012, the Federal Communications Commission (FCC) conducted an inquiry in the wake of a derecho storm that left millions without electricity for extended periods of time and impacted 911 services. Industry trade group CTIA –The Wireless Association's response to this inquiry illustrates the wireless industry's current efforts to ensure resiliency and reliability in case of extreme weather events (CTIA, 2012). It cites the efforts of wireless providers, including Verizon and AT&T, in building redundant networks, employing portable or temporary base stations to provide network continuity, using back-up sources of power, tailoring network resiliency and continuity of service plans to the unique needs of individual localities, and employing network management techniques to address spikes in traffic likely to occur during an emergency (ibid.). All of these types of initiatives have been recommended in the literature as adaptation options. Thus the current plans and processes of telecommunications operators in responding to weather-related emergencies provide a good starting point from which to incorporate long-term climate change considerations, including an increased frequency of extreme events as well as incremental change such as temperature rise. Current responses provide "the basis for adaptability in the future" (Horrocks et al., 2010).

However, it is important to note that the FCC's final report on the subject does not necessarily support the CTIA's. The FCC stated that the derecho provided a snapshot of the reliability and readiness of part of the US communications infrastructure in the face of unanticipated disasters and highlighted flaws in the resiliency planning and implementation of the 911 network providers. The investigation found that, in most cases, the disruptions could have been avoided if network providers had fully implemented best industry practices based on available guidance. This illustrates that while guidance on potential resilience building measures exists, implementation remains another issue.

Gap analysis

This section shares insights on knowledge gaps and barriers as identified in the literature scan.

Knowledge gaps

The literature scan revealed significant gaps in terms of available data and knowledge on climate change impacts and risks in both sectors. Many expected impacts are speculative and few are assessed in detail in the technical or scholarly literature. The evidence for climate change adaptation in both industries primarily comes from the drive to improve energy and (in data centers) water efficiency. However, while there is some analysis of how existing hazards could impact operations, future conditions are not taken into consideration.

Comparing UK and US domestic policy suggests there is less knowledge of, and less priority given to, the telecommunications sector in the US in terms of understanding or addressing climate change risk. The recent US National Climate Assessment does not refer to the sector in any detail, while the UK Climate Change Risk Assessment contains a section on climate change risk to the ICT sector, highlighting its importance for all industries in the UK.

Much of the literature on risk and resilience in both sectors cites severe weather events as threats of significant concern (for example, see BCI, 2013 and ClimAID, 2011). However, there is hardly any mention of climate change in this context. For example, Ernst and Young (2012) have published the top 10 business risks to telecommunications, which does not feature weather or climate impacts. In contrast, BT's former CEO, Ian Livingston, has stated that climate change threatens economic prosperity and business profitability, which is clearly illustrated in BT's own experience with flooding (Acclimatise, 2013). There appears to be a gap between what is being reported and what is increasingly being experienced.

In the US, as of 2011, "the [telecoms] industry generally lacks computerized databases that readily show the location and elevations of installed telecommunication facilities and lifelines and their operational capacity. Such data can be crucial in extreme weather events to make rapid damage, loss, and consequence assessments in potential hazard and damage zones" (ClimAID, 2011).

Although there are several historical case studies relating to weather-related disruptions to telecommunications and data centers (several of which are included above), these tend to be isolated and poorly documented.

There is an absence of publicly-available, quantitative information on the costs of climate risks, though many companies may not hold this information internally either. Examples of missing information include damage costs, increases in operational maintenance costs, number of customer disruptions, and insurance claims by companies (making claims on damage to assets).

The evidence suggests that the siting of data centers may become increasingly dependent on access to cool air for free air cooling systems; for example, HP has just opened a new data center on the north coast of the UK to access cooler air temperatures for this purpose. The deployment of data centers off-shore and in cooler climates (primarily northern latitudes) is also expected. However, while addressing the immediate issue of energy and water supply, these centers may also be at risk from climate change, in relation to rising sea levels, extreme weather, or melting permafrost (Horrocks et al., 2010). Ensuring that the decisions made in respect to data centers now are robust against a range of possible future (uncertain) climates is a key missing element in this discourse.

There is little evidence of climate change risk assessments of the sector's interaction with energy, which is a crucial and often vulnerable input. There appears to be equally little dialogue between the energy and ICT sector as well despite their inter-linkages (URS, 2010).

Barriers and limitations to leverage existing resources

- Robust data is currently not available in most countries to provide a meaningful assessment of potential climate change impacts across the range of assets and infrastructure common to telecommunications and data centers services systems (Baglee et al., 2012). This gap is particularly noticeable when compared to the greater level of information on climate risks in other sectors, notably in energy, transportation, and water.
- Lack of quantitative data demonstrating material value of building resilience, combined with the fact that there are no

studies that model the scale and cost of future events on the data centers or telecommunications sectors, means that there is currently a weak business case for spurring action on climate risk. This lack of information is due in part to confidential business information surrounding past events, as well as the challenge of avoiding losses avoided as a result of successfully implemented resilience-building activities.

- Insufficient data in technical or scholarly literature on how changes in weather extremes and in climatic averages affect technical components and bespoke infrastructure in both sectors.
- There is limited awareness or understanding of climate risks in telecommunications and data centers globally. There is similarly little insight on potential costs of a changing climate, an awareness that would drive greater investigation into key vulnerable relationships like that with energy.
- Insufficient consideration of future climate change in decision-making generally, and in the telecommunications sector specifically.
- Lack of case studies demonstrating the business case for resilience.
- Lack of regulation in US to enforce resilience (especially when comparing US to UK regulation/policy).

4. Summary and Recommendations

This section summarizes the key risks and opportunities from this report, and points to some recommendations for next steps to build upon this work.

Key risks and vulnerabilities

Poor understanding of risks to supply chains. Our team believes the supply chain maps indicate where we should look for climate risks, but the literature does sufficiently describe supply chain risks. While supply chain risks are both intuitively significant and have had their significance documented in analogous sectors (such as energy production, transmission, and distribution), the focus in the literature is on climate risks to infrastructure to the near exclusion of enterprise supply chains and critical inputs such as water and electricity.

Lack of attention given to slow-onset change. More focus is given to 'headline' climate events (such as extreme storms) rather than to the slower, less dramatic climate shifts (for example, increasing ambient air temperatures) reducing asset performance headroom and operational efficiency that can have similarly serious consequences for infrastructure and equipment.

Centralization of assets. The security and technological benefits of reducing the total number of data centers (as is, for example, currently underway by the US Government) may be countered by the disadvantage of reduced redundancy in a system faced with increasing climate risk. This risk is also seen in the growing tendency and regulatory framework that encourages telecom providers to share infrastructure.

Technological heterogeneity. As telecoms move away from landlines and cable-based technologies to build wireless systems, this may mean that companies invest less in the operational maintenance of landlines. For remote/rural communities, this could mean that their systems are less maintained, which could increase asset vulnerability to extreme events.

Risks to power generation and distribution. Though the electricity sector is critical to both sectors and itself susceptible to climate risk, the inter-linkages between the two remain poorly defined. Reliable access to power, particularly in times of extreme weather, remains a significant risk to telecommunications and data centers.

Key opportunities

Shared infrastructure allows for shared resilience. Though there is reduced redundancy, climate resilience may be more readily addressed as there are fewer, more concentrated ICT assets in both sectors.

Companies can share best practice. Growing cooperation between companies in the same sector sharing infrastructure may provide an incentive to share climate risk mitigation techniques that may contribute to the resilience of the sector as a whole.

High turnover of technology creates opportunities to spread best practice. ICT technology is rapidly evolving, providing businesses with frequent opportunities to replace and upgrade equipment that is more resilient.

Raise awareness. Recent extreme events and their impacts on telecoms and data centers have led to some incremental gains in awareness among providers and the government. These events create windows of opportunity to engage experts and stakeholders to collect better/more information as well as creating interest in allocating funding for research. Extreme events, and the consequences for the sectors together with the responses undertaken (if well documented), can be captured as case studies used to demonstrate the business value to other companies in building resilience.

Harmonize resilience building activities with sustainability efforts. Where alternative water and energy sources have been sought there should be an evaluation as to whether they are resilient to future climates. Likewise, there is significant momentum in both sectors toward increasing energy efficiency of facilities and technology, efforts that could dovetail with resilience.

Build on work done in the energy sector. Electricity generation, transmission, and distribution is a high climate risk sector that has been more extensively studied than telecommunications. It is also, as a sector, analogous to telecommunications in terms of its networked infrastructure and critical role to other sectors. Finally, power is a vital input to both telecoms and data centers. Climate risk to telecommunications should both build on insights learned from the energy sector as well as account for their inter-linkages.

Recommended actions

The absence of evidence in the literature on supply chain risks in both sectors limits the scope of recommendations that can be made. Further foundational research and consultations are required to assess supply chain disruptions, protect return on investment, and increase the ability of the federal government to work with vendors to address climate risk. Some initial recommendations are described below.

Frame climate risks as business risks. The literature scan above categorizes climate risks as they were generally presented in the literature: according to climate variables such as temperature and rainfall. However, it is more effective to organize climate impacts against business functions. This approach contextualizes climate risk in the perspective of private sector companies, their customers, investors, and regulators. The supply chain maps provide a framework toward presenting useful technical insights gleaned from the literature scan in the context of the actual assets, operations, and relationships that make up these sectors.

Plan for a changing climate baseline and for climate extremes. Storms and other examples of extreme weather grab headlines and can lead to action, but incremental climate change can subtly shift the baseline and lead to long-term system failures. Successfully addressing climate risk requires careful attention to subtle impacts (e.g., the cumulative impact of increasing sequences of warmer than average days on wired telecommunications) as well as to the effects of storms and floods.

Build awareness of climate risks before disasters strike. Adaptation to climate risks depends upon awareness and/or action by three groups of stakeholders: telecommunications infrastructure and service providers, customers reliant on telecommunications services, and government facilitators of the market demand for climate resilience (Horrocks et al., 2010). Working with all three sets of stakeholders to build consensus and collect the information each offers is required to effectively build resilience,

Conduct direct consultations with the private sector. "Adapting the ICT sector to the impacts of climate change" by Horrocks et al (2010) was the most useful piece of literature discovered and a significant resource in the preparation of this report. Its limitations here were that it was UK focused (thus focused on a narrower spectrum of possible climates than in the US) and encompassed all of ICT, of which telecoms and data centers are only a part. However its most useful contribution may be the focus on engagement direct with industry stakeholders rather than with the public sector. Conducting similar sectoral consultations with a US-focus, utilizing surveys, interviews, and/or workshops with executives, engineers, designers, and other experts, is a clear first step towardunderstanding likely impacts and adaptation options. Working with these key stakeholders, who know the business, sites, and technologies better than anyone, will involve speaking the language of their sector and harnessing their expertise to understand what would happen under likely climate scenarios. It would be an opportunity to frame existing and project climate perils in the terms of the private sector, and capture their exclusive knowledge of their own business.

Thoroughly assess climate risks of both telecoms and data center sectors. A full climate risk assessment, informed by consultations with experts and stakeholders, would allow for the prioritization of risks to both sectors according to their relative consequence and likelihood. Such an assessment would also address a gap found in the literature regarding the absence of discussion on enterprise supply chain risks to the sectors.

Require federal service providers in both sectors to demonstrate climate resilience. Federal agencies should include provisions in all their procurement processes requiring suppliers to undertake a climate risk assessment and demonstrate how their products/services will continue to meet required contractual and serviceability performance standards given the potential impacts of a changing climate (including those affecting their suppliers (e.g. electricity utilities).

Elucidate, test, and document adaptation practice as value protection strategies. The literature scan turned up a number of promising adaptation options for strengthening the resilience of business assets and operations. However, these options were poorly explained or defined, and most were not tied to case studies sharing lessons learned from implementation. There is a clear gap, particularly in the US market, for expanding on this nascent body of knowledge.

Prepare a comprehensive technical study to develop headroom analyses for key assets in both sectors. From this review of the literature, it is clear that there is currently limited understanding of the critical thresholds at which telecom and data center assets may be affected by extreme events. It is also clear that understand is very limited about the thresholds at which the sectors are affected by incremental change. A comprehensive study into the functional thresholds for critical assets would assist in identifying and prioritizing risks, planning operational maintenance, and informing future capital expenditures. Once there is better understanding of infrastructure and equipment operating headrooms, businesses will also be better prepared to identify and evaluate different adaptation actions. As seen in **Figure 5**, adaptation allows for maintaining operating headroom in a changing climate by increasing the critical threshold or coping range to allow an asset or system to withstand the effects of a changing climate.

Assess telecoms and data centers within the context of their feasible lifetimes. Horrocks et al. (2010) mention how data centers might be affected by higher temperatures in 2080. This distant timeframe, which is brought up in several of the resources reviewed, is largely irrelevant given the short generational cycles of ICT technology, and as the current systems in use will likely be fully replaced by 2080. It is necessary to, in consultation with technology experts, align the expected life cycles of technology in both sectors with relevantly scaled climate risk assessments, to ensure that assets are robust and protected throughout the timeframe of their useful life.

Include telecoms and data centers in the fourth National Climate Assessment (NCA). Released in Summer 2014, the third NCA was a major step forward in the articulation of climate risks to key sectors in the US Given the integral role of ICT sectors, these should be included in the next NCA.

Provide guidance to ICT companies in these sectors on material risk disclosure to the Securities Exchange Commission (SEC, 2010). All companies operating in these sectors are at risk from challenges by their investors seeking risk disclosures. Specific sectoral guidance should be prepared (developed in consultation with institutional investors and trade associations), setting out how a risk assessment should be undertaken and the issues to be disclosed.

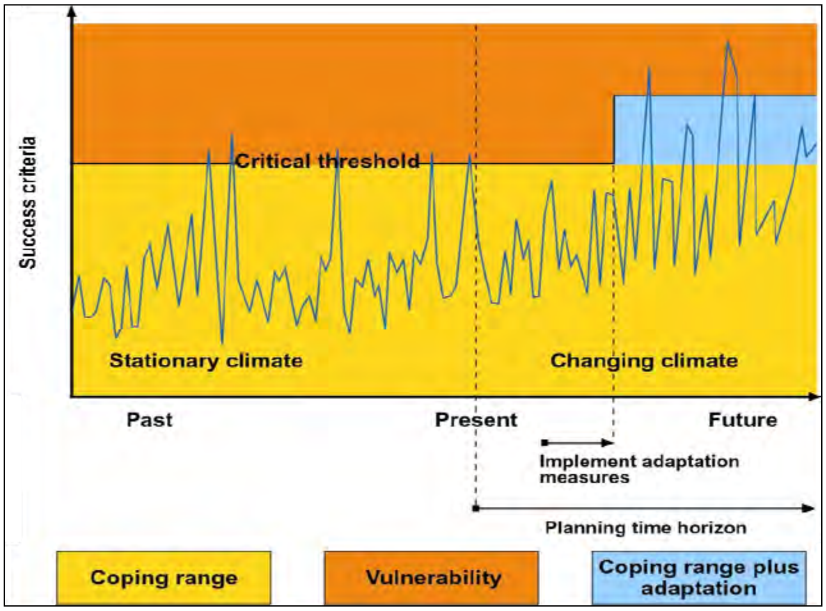


Figure 5 – Effects of adaption on the critical threshold or coping range of systems and assets to withstand impacts in a changing climate (Willows and Connell, 2003)

5. Annotated Bibliography

All literature sources are captured in the References section at the end of the report. Those references that substantially address the topic are also catalogued in this Annotated Bibliography.

Acclimatise. (2008) *Climate change risks to data centers.* Acclimatise Business Intelligence report, from http://www.acclimatise.uk.com/login/uploaded/resources/__Acclimatise_DataCentres.pdf

This short report summarizes key climate change risks to data centers, as well as the importance of assessing interactions between climate hazards and other risk factors. It also provides several case studies illustrating climate impacts on data centers and suggests risk management measures and opportunities that may arise due to climate change.

Baglee, A., Haworth, A. & Anastasi, S. 2012, *UK Climate Change Risk Assessment (CCRA) for the Business, Industry and Services Sector*. London: Department for Environment, Food and Rural Affairs (Defra) from http://randd.defra.gov.uk/Document.aspx?Document=CCRASummaryBusinessIndustryandServices.pdf

This report uses available evidence and expert opinion to consider the effects of climate change for the business, industry, and services sector. The aim of the CCRA is to help the UK government prioritize and implement necessary adaptation measures. One of the risks identified to the sector as a whole is an associated with a decrease in productivity and revenues due to ICT loss/ disruption. The report also points out there is little suitable literature that specifically considers the potential impacts of climate change on ICT and cascading effects to other businesses.

Carbon Disclosure Project (CDP) 2012, *Insights into Climate Change Adaptation by UK Companies*. London: CDP. Available from: http://archive.defra.gov.uk/environment/climate/documents/cdp-adaptation-report.pdf [accessed 1 August 2014].

This report analyzes data submitted by members of the FTSE 100 (89 companies in total) in response to CDP information requests from 2011 in order to gather insights into business attitudes and actions on adaptation. Telecommunications is represented as a sector and associated risks and opportunities identified from corporate disclosure documents; however, only two telecommunications companies reported to CDP. The report also features a case study of British Telecom (BT), which provides detailed information on the company's activities to adapt to climate change, one of the most comprehensive case studies of corporate resilience in the telecommunications sector available.

Carbon Disclosure Project (CDP) 2011, *Telecommunications sector report*. London: Author. Available from: https://www.cdproject.net/CDPResults/2011-G500-sector-report-telecommunicationsmunications.pdf [accessed 1 August 2014].

This report summarizes responses to the 2011 Carbon Disclosure Project Information Request from Telecommunications companies in the FTSE Global Equity Index Series, Standard & Poor's 500 Index, and the FTSE 350 Index. It highlights climate change risks and opportunities as reported by companies, with quotes illustrating examples of current action on climate change and attitudes toward climate policy. Examples are primarily focused on reducing emissions, with some mention of addressing physical climate impacts.

CSIRO 2006, *Climate Change and Infrastructure: Planning Ahead*. Melbourne: Victorian Government from http://www.climatechange.vic.gov.au/__data/assets/pdf_file/0018/73242/ClimateChangeandInfrastructureSummary.pdf

Recognizing that infrastructure represents a large, long-term investments and that much of it is built, designed, and operated based on historical climate information, this short report highlights the importance of examining climate risks in order to plan for future climate change. It examines potential risks to various infrastructure types, including telecommunications, due to likely future climate change in Victoria, Australia, using worst case scenarios for 2030s and 2050s. The report

finds, among other results, greater risk to the fixed line telecom network than to the mobile network.

CTIA – The Wireless Association (2012) "Comments of CTIA – The Wireless Association before the Federal Communications Commission (FCC), Washington, D.C. 20554, in the matter of: Comment Sought on 911 Resiliency and Reliability in Wake of June 29, 2012, Derecho Storm in Central, Mid-Atlantic, and Northeastern United States." Available from: http://www.ctia.org/docs/default-source/fcc-filings/ctia-comments-on-911-resiliency-and-reliability-in-the-wake-of-the-june-29-2012-derecho-storm.pdf?Status=Master&sfvrsn=0 [accessed 30 July 2014].

This comment submitted to the FCC outlines the wireless industry's opposition to the imposition of any "one-size-fits-all" procedures and regulations on wireless carriers in order to maintain resiliency and reliability of 911 communications. This was prompted by a particularly destructive storm that resulted in large power outages, which prompted discussion about regulation to prevent further occurrences in the future. The authors claim that the FCC should adopt a flexible approach, and that voluntary efforts will lead to the development and utilization of highly effective resiliency and reliability solutions. They also illustrate existing efforts of the wireless industry to promote continuity of service and network resiliency, and how it continues to develop disaster readiness and recovery practices.

Department of Energy (DOE). (2014a) The Water-Energy Nexus: Challenges and Opportunities. http://energy.gov/downloads/water-energy-nexus-challenges-and-opportunities

This report explains the interrelationship between water and energy and its importance to the energy sector. It calls for a more integrated approach to address the challenge and opportunities around the water-energy nexus. It highlights the DOE's expertise in technology, modeling, data and analysis, which could contribute to further understanding of the nexus and provide potential solutions. Six strategic pillars are identified that will serve as the foundation for addressing the water-energy nexus.

Department of Energy (DOE), 2014b. Liquid Cooling v. Air Cooling Evaluation in the Maui High Performance Computing Center. http://energy.gov/eere/femp/downloads/case-study-evaluating-liquid-versus-air-cooling-maui-high-performance-computing

This paper describes the efficiency characteristics of a water cooled information technology (IT) system applied in a retrofit project at the Maui High Performance Computing Center data center. An evaluation of cooling and electrical system components during system tests showed much less cooling power is required by the water cooled IT system, compared to the cooling power required by the air cooled system. It is estimated that the water cooling will save $200,000 per year in operating costs.

Defra. (2011) *Climate Resilient Infrastructure: Preparing for a Changing Climate*. Retrieved August 5, 2014 from https://www.gov.uk/government/publications/climate-resilient-infrastructure-preparing-for-a-changing-climate

This report is a response to calls from industry - infrastructure owners, investors and insurers - for a government vision and policy on adapting infrastructure to climate change. It is primarily designed to catalyze action to adapt sectors with infrastructure networks, including in the energy, ICT, transportation, and water sectors. It identifies relevant actors as well as associated challenges and opportunities. Recognizing how much infrastructure is private sector funded and operated, it sets out how the UK government can assist others in realizing an infrastructure network that is able to adapt to the impacts of climate change.

Engineering the future. (2011) Infrastructure, engineering and climate change adaptation – ensuring services in an uncertain future. The Royal Academy of Engineering. Retrieved August 5, 2014 from http://www.raeng.org.uk/publications/reports/engineering-the-future

This report examines vulnerabilities in different sectors of the UK national infrastructure to the effects of climate change and the modifications that would be required to increase resilience. It also considers vulnerabilities that affect the infrastructure system as a whole and which arise as a result of interdependencies between different sectors. This study, intended to feed into a UK cross-government Infrastructure and Adaptation project, was carried out from the perspective of the engineering profession and the engineering response to the demands of climate change adaptation. It was based on consultations from workshops which brought together stakeholders from four infrastructure sectors: energy, transport, water and communications.

Garnaut Climate Change Review. (2008) *Impact of Climate Change on Australia's Telecommunications Infrastructure*. Melbourne: Cambridge University Press. http://www.garnautreview.org.au/CA25734E0016A131/WebObj/02-CTelecommunications/$File/02-C%20Telecommunications.pdf

The Garnaut Review was an independent study commissioned by the Australian government on the impacts of climate change on the Australian economy. This particular section of the report reviews the impacts on telecommunication infrastructure, under seven different climate scenarios, for the 2030s, 2070s and 2100s. The report adopts an economic lens, describing impacts in terms of their effect on operational and capital expenditures.

Horrocks, L, Beckford, J, Hodgson, N, Downing, C, Davey, R and O‟Sullivan, A. (2010) *Adapting the ICT Sector to the Impacts of Climate Change – Final Report*, Defra contract number RMP5604. London: Defra from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/183486/infrastructure-aea-full.pdf

This report presents the findings of a scoping study to explore the impacts of climate change on the UK ICT sector and the potential for adaptation. It was undertaken as part of a UK government program for adapting national infrastructure. This is the most comprehensive report of its kind on climate risks in the ICT sector, exploring climate change impacts and their implications for ICT and in its relationships to other sectors, how the sector can adapt, identifies factors that drive and constrain adaptation, and concludes with suggestions. The authors find that while ICT providers are able to respond to weather events, there is still little awareness of climate change risk, and little evidence that key ICT companies and organizations adopt appropriate climate risk management or adaptation strategies. The report is focused on the UK ICT sector, which limits generalization beyond the UK; however, the authors have recognized the global nature of the industry and make references to it where appropriate. One limitation is that the authors emphasize that changes in the nature and frequency of extreme events are of most concern, rather than long-term average increases, potentially missing implications of long-term incremental climate impacts.

Jacob, K., Maxemchuk, N., Deodatis, G., Morla, A., Schlossberg, E., Paung, I., Lopeman, M., Horton, R., Bader D., Leichenko, R., Vancura, P., & Klein Y. 2011, Ch. 10: Telecommunications. Responding to Climate Change in New York State: The ClimAID Integrated Assessment for Effective Climate Change Adaptation in New York State, C. Rosenzweig, W. Solecki, A. DeGaetano, M. O'Grady, S. Hassol, and P. Grabhorn, Eds., New York State Energy Research and Development Authority (NYSERDA), 363-396zfrom http://www.nyserda.ny.gov/-/media/Files/Publications/Research/Environmental/EMEP/climaid/ClimAID-Telecommunications.pdf

This chapter forms part of an integrated assessment for climate change adaptation in New York State intended to help public and private decision-makers create effective adaptation strategies. It focuses exclusively on telecommunications. It explores the main climate impacts in the context of New York State's telecommunications sector, which the report characterizes as primarily privately owned and closely connected to the energy sector. It suggests adaptation options, from the technical to the strategic, and highlights co-benefits. A unique contribution of this report is that it explores impacts on particularly vulnerable groups, such as those in rural areas or lower-income, elderly, or disabled populations. It also illustrates potential climate impacts through a case study of a hypothetical composite of historical extreme winter storms. In terms of the effects of climate change, framed as vulnerabilities and opportunities, the authors focus primarily on the impact of extreme events, neglecting long-term climate change.

Kelly, T. & Adolph, M. 2008, ITU-T Initiatives on Climate Change, *IEEE Communications Magazine*. 46(10), 108-114 from http://ieeexplore.ieee.org/xpl/abstractKeywords.jsp?arnumber=4644127

This article looks at the potential role ICTs play in terms of its relationship to climate change, from how it contributes greenhouse gas emissions to how ICT can be used to monitor it. It also looks to ways of developing long-term solutions to mitigate and adapt to climate impacts, both directly in the ICT sector and in other sectors such as energy, transport, and buildings. A small section of the article is devoted to adaptation efforts; however, these are focused on how ICT can enable adaptation, not how the sector itself is adapting.

Office of Communications (Ofcom) (UK) 2011, C*limate Change Adaptation: Impact on our functions. A Response to the Secretary of state’s Direction of 31 March 2010*. London: Ofcom. Available from: http://www.ofcom.org.uk/binaries/consultations/ofcomresponses/Climate-change-adaptation.pdf [accessed August 5, 2014].

This report summarizes Ofcom’s functions and assesses the possible impacts of climate change in relation to these functions. The report notes the challenges in assessing climate impacts due to limited information (much of it being held by individual network operators), the uncertainty of climate projections, and the rapidly changing nature of technology in the industry. It set out some of the areas where climate change could affect the sector in the future, including impact on infrastructure, use of the radio spectrum, and Ofcom’s operations, as well as the mechanisms that already exist to consider such developments. It also sets out how Ofcom as an organization will maintain its ability to adapt to climate change.

Ospina, A.V., Faulkner, D., Dickerson, K. & Bueti, C. (2014) *Resilient Pathways: the adaptation of the ICT sector to climate change*. Geneva: International Telecommunication Union (ITU). http://www.itu.int/en/ITU-T/climatechange/Documents/Publications/Resilient_Pathways-E.PDF

The main objective of this report is to explore the impacts of climate change on the ICT sector and the potential for adaptation, while emphasizing the need for resilient pathways of action, enabling environments, and new standards to foster the sector’s approach to adaptation. The report presents an overview of climate impacts, opportunities and challenges posed by climate change, the sector’s response to climatic impacts, identifying existing and emerging adaptive strategies, and suggesting areas for future action. The analysis includes examples identified through a survey conducted among key sector stakeholders involved in ICT, environmental sustainability, and climate change strategies. A unique feature of the report is that is applies a resilience lens to the sector’s approach to adaptation. It goes beyond contingency and risk management, proposing pathways that allow the sector to identify and implement actions to manage short-term risks, as well as respond flexibly to future impacts.

Quanta Technology 2009, *Cost-Benefit Analysis of the Deployment of Utility Infrastructure Upgrades and Storm Hardening Programs*. Available from: http://www.puc.texas.gov/industry/electric/reports/infra/utlity_infrastructure_upgrades_rpt.pdf [accessed August 8 2014]

This report examines the costs, utility benefits, and societal benefits of a variety of storm hardening programs for utilities, including in the ICT sector. The authors find that certain targeted vegetation and hardening approaches can be cost-effective, especially if they are based on detailed post-storm data collection and analyses. The report includes an analysis of the telecommunications utility sector, looking at the associated costs of hurricanes and tropical storms, as well as examples of what companies are doing to reduce such costs.

UK Climate Impacts Programme (UKCIP) 2013, *Ofcom’s fixed asset market review – overview of climate change impacts*. Oxford: UKCIP from http://stakeholders.ofcom.org.uk/binaries/consultations/fixed-access-market-reviews/responses/Openreach_-_UKCIP_report.pdf

This report was authored by UKCIP for Openreach, the infrastructure division of British Telecom (BT) Group. It describes the current scientific and policy landscape for climate impacts and adaptation in the UK, including the extent to which climate change has been considered by the telecommunications sector. It considers how other sectors (and regulators) have responded to the challenge of climate change and describes the likely changes the UK will face, based on the best available projections. The report concludes with recommendations for future research to examine how these changes may impact on the ability of Openreach to maintain business

continuity and service quality in a changing climate. The report highlights the challenge that there is limited public information on how the telecommunications sector will be impacted by climate change.

URS 2010, *Adapting Energy, Transport and Water Infrastructure to the Long-term Impacts of Climate Change*, UK cross-departmental Infrastructure and Adaptation project, contract no. RMP/5456 from http://archive.defra.gov.uk/environment/climate/documents/infrastructure-full-report.pdf

This report presents the case for adapting infrastructure in the energy, transport, and water sectors. The report focuses on the long-term impacts of climate change (2030s to 2100), setting out the risks to the three types of infrastructure, the interdependency of risks within the infrastructure system, adaptation options, and barriers to action. It also provides recommendations to the Infrastructure and Adaptation project that commissioned the report. The section on interdependencies refers to ICT (p. 66), outlining the relationship of each sector to ICT, suggesting that interdependencies can increase vulnerability to climate change and must be considered systematically in the assessment of climate risks. This report underpins the idea that ICT is a critical sector to all others, and one whose resilience will have a wider positive effect. It also points out that there are few climate change risk assessments for the ICT sector.

Wong, J., & Schuchard, R. 2011*, Adapting to Climate Change: A Guide for the ICT Industry*. Business for Social Responsibility (BSR) from http://www.bsr.org/reports/BSR_Climate_Change_Adaptation_ICT.pdf

This guide for businesses illustrates how ICT companies are reporting on climate change risks and opportunities, based on an analysis of Carbon Disclosure Project (CDP) responses of 133 companies. It outlines current and emerging best practices, framed as either value protection or value creation. Examples of best practice are based on CDP disclosures, interviews, and a literature review. The authors recognize that current best practice, comprised primarily of technical and management techniques, is limited. They offer guidance on formulating a proactive approach to adaptation, suggesting that companies develop adaptation strategies to prepare for the rising unpredictability and severity of future climate change impacts. The report concludes with recommendations for key components of these adaptation strategies. The report's main strength is that it showcases many case studies and examples of how companies are responding to climate variability and change, providing early basis for the formulation of good practice principles.

6. References

Acclimatise. (2008) *Climate change risks to data centers.* Acclimatise Business Intelligence report, from http://www.acclimatise.uk.com/login/uploaded/resources/__Acclimatise_DataCentres.pdf

Acclimatise (June 2013). Climate change calling: BT CEO says climate change is a risk to UK Plc. Retrieved August 5, 2014 from http://www.acclimatise.uk.com/network/article/climate-change-calling-bt-ceo-says-climate-change-is-a-risk-to-uk-plc

Alger, D. (2005) Choosing an optimal location for your data center. *Cisco Press.* Retrieved 5 August, 2014 from http://www.ciscopress.com/articles/article.asp?p=417091

Arrieta, F.P. & Lora, E. E. S. (2005) Influence of ambient temperature on combined cycle power-plant technology. *Applied Energy*. 60 (3). p. 261-272. http://ideas.repec.org/a/eee/appene/v80y2005i3p261-272.html

Baglee, A., Haworth, A. & Anastasi, S. 2012, *UK Climate Change Risk Assessment (CCRA) for the Business, Industry and Services Sector*. London: Department for Environment, Food and Rural Affairs (Defra) from http://randd.defra.gov.uk/Document.aspx?Document=CCRASummaryBusinessIndustryandServices.pdf

BEA (2007) "Use Tables / After Redefinitions / Producer Value", Department of Commerce, from http://www.bea.gov/industry/xls/IOUse_After_Redefinitions_PRO_2007_Detail.xlsx

Brill, K.G. and Stanley, J. (2009) IT and Facilities Initiatives for Improved Data Center Energy Efficiency. *Uptime Institute*. Retrieved 6 August, 2014 from http://uptimeinstitute.com/publications

Business Continuity Initiative (BCI). (November 2013). *5th Annual Survey: Supply Chain Resilience*. BCI. Retrieved 29 September, 2014 from http://www.zurich.com/internet/main/sitecollectiondocuments/reports/supply-chain-resilience-2013-en.pdf

CDP. (2010) *Telecommunications Sector Report*. London: CDP from https://www.cdp.net/CDPResults/CDP-2010-Sector-Report-Telecommunications.pdf

CDP. (2012) *Insights into Climate Change Adaptation by UK Companies*. London: CDP from https://www.cdp.net/CDPResults/insights-into-climate-change-adaptation-by-uk-companies.pdf

CDP. (2014) *Climate change resilience in Europe: A snapshot of the private sector*. London: CDP. from https://www.cdp.net/CDPResults/climate-change-resilience-europe.pdf

Chestney, N. (2013) Business looks to UN report for clarity on climate risks. *Reuters*. Retrieved August 5, 2014 from http://www.reuters.com/article/2013/09/26/climate-ipcc-business-idUSL5N0HF31U20130926

CSIRO (2006), *Climate Change and Infrastructure: Planning Ahead*. Melbourne: Victorian Government from http://www.climatechange.vic.gov.au/__data/assets/pdf_file/0018/73242/ClimateChangeandInfrastructureSummary.pdf

CTIA – The Wireless Association. (2012) Comments of CTIA – The Wireless Association before the Federal Communications Commission, Washington, DC 20554, in the matter of: Comment Sought on 911 Resiliency and Reliability in Wake of June 29, 2012, Derecho Storm in Central, Mid-Atlantic, and Northeastern United States. Retrieved 30 July, 2014 from http://www.ctia.org/docs/default-source/fcc-filings/ctia-comments-on-911-resiliency-and-reliability-in-the-wake-of-the-june-29-2012-derecho-storm.pdf?Status=Master&sfvrsn=0

Darrow, K. and Hedman, B. (2009) Opportunities for Combined Heat and Power in Data Centers. Centre of Expertise for Energy Efficiency in Data Centers. Retrieved 5 August, 2014 from http://datacenters.lbl.gov/resources/opportunities-combined-heat-and-power-data-centers

Defra. (2011) *Climate Resilient Infrastructure: Preparing for a Changing Climate*. Retrieved August 5, 2014 from https://www.gov.uk/government/publications/climate-resilient-infrastructure-preparing-for-a-changing-climate

Department of Energy (DOE). (2014a) *The Water-Energy Nexus: Challenges and Opportunities*. Retrieved August 5, 2014 from http://energy.gov/downloads/water-energy-nexus-challenges-and-opportunities

Department of Energy (DOE), (2014b) *Liquid Cooling v. Air Cooling Evaluation in the Maui High Performance Computing Center.* http://energy.gov/eere/femp/downloads/case-study-evaluating-liquid-versus-air-cooling-maui-high-performance-computing

Emerson Network Power. (2011) *Understanding the Cost of Data Center Downtime: An Analysis of the Financial Impact on Infrastructure Vulnerability.* Retrieved August 5, 2014 from http://www.emersonnetworkpower-partner.com/ArticleDocuments/SL-24661.pdf.aspx?Embed=Y

Engineering the future. (2011) Infrastructure, engineering and climate change adaptation – ensuring services in an uncertain future. The Royal Academy of Engineering. Retrieved August 5, 2014 from http://www.raeng.org.uk/publications/reports/engineering-the-future

EPA. (2007) Report to Congress on Server and Data Center Energy Efficiency Public Law 109-431. US Environmental Protection Agency ENERGY STAR Program. Retrieved 11 August, 2014 from http://www.energystar.gov/index.cfm?c=prod_development.server_efficiency_study

Garnaut Climate Change Review. (2008) *Impact of Climate Change on Australia's Telecommunications Infrastructure*. Melbourne: Cambridge University Press. http://www.garnautreview.org.au/CA25734E0016A131/WebObj/02-CTelecommunications/$File/02-C%20Telecommunications.pdf

Goldman, D. (2012) Cell phone carriers brace for Hurricane Sandy. *CNN Money*. Retrieved August 8, 2014 from http://money.cnn.com/2012/10/29/technology/mobile/cell-phone-sandy/index.html

Google. (2014). *From paper mill to data center*. Retrieved August 5 from https://www.google.com/about/datacenters/inside/locations/hamina/

GSA. (2012). FY 2013 Climate Change Adaptation Action Plan. US General Services Administration. June 2012.
http://www.gsa.gov/portal/mediaId/162947/fileName/Climate_Change_Adaptation_Action_Plan_FY13

Horrocks, L, Beckford, J, Hodgson, N, Downing, C, Davey, R and O"Sullivan, A. (2010) *Adapting the ICT Sector to the Impacts of Climate Change – Final Report*, Defra contract number RMP5604. London: Defra from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/183486/infrastructure-aea-full.pdf

IPCC (2014). 5th Assessment Report, Working Group II, Chapter 8. Retrieved 5 August, 2014 from http://ipcc-wg2.gov/AR5/images/uploads/WGIIAR5-Chap8_FGDall.pdf

Jacob, K., N. Maxemchuk, G. Deodatis, A. Morla, E. Schlossberg, I. Paung, M. Lopeman, R. Horton, D. Bader, R. Leichenko, P. Vancura, and Y. Klein. (2011) Ch. 10: Telecommunications. *Responding to Climate Change in New York State: The ClimAID Integrated Assessment for Effective Climate Change Adaptation in New York State*, C. Rosenzweig, W. Solecki, A. DeGaetano, M. O'Grady, S. Hassol, and P. Grabhorn, Eds., New York State Energy Research and Development Authority (NYSERDA), 363-396 from http://www.nyserda.ny.gov/-/media/Files/Publications/Research/Environmental/EMEP/climaid/ClimAID-Telecommunications.pdf

Kahn, B. (November 4, 2012) Superstorm Sandy and Sea Level Rise. NOAA Climate.gov. Retrieved August 11, 2014 from http://www.climate.gov/news-features/features/superstorm-sandy-and-sea-level-rise

Kelley, C., Singh, H., Smith, V. (2013) Data center efficiency and it equipment reliability at wider operating temperature and humidity, Strutt, S., Ed. White Paper #50, The Green Grid from http://www.thegreengrid.org/~/media/WhitePapers/WP50-Data%20Center%20Efficiency%20and%20IT%20Equipment%20Reliability%20at%20Wider%20Operating%20Temperature%20and%20Humidity%20Ranges.pdf?lang=en

Kelly, T. & Adolph, M. 2008, ITU-T Initiatives on Climate Change, *IEEE Communications Magazine*. 46(10), 108-114 from http://ieeexplore.ieee.org/xpl/abstractKeywords.jsp?arnumber=4644127

NASA. (2012) *Adapting Now to a Changing Climate: Stennis Space Center*. Accessed August 5, 2014 from http://www.hq.nasa.gov/office/codej/codejx/Assets/Docs/NASA-Stennis_Climate%20Info_web.pdf

Mahdavi, R. (2014) *Case Study: Opportunities to Improve Energy Efficiency in Three Federal Data Centers*. Lawrence Berkeley National Laboratory US Department of Energy's Federal Energy Management Program.
http://energy.gov/sites/prod/files/2014/06/f16/casestudy_3federaldatacenters_0.pdf

Marketwired. (August 26, 2014) *UGE Secures Order to Power Telecoms Sites With Distributed Renewable Energy Microgrids*. Retrieved September 1, 2014 from: http://www.marketwired.com/press-release/uge-secures-order-power-telecoms-sites-with-distributed-renewable-energy-microgrids-tsx-venture-ug-1941443.htm

Miller, R. (2013) *Activists Target Water Supply for NSA Data Center*. Data Center Knowledge. Retrieved August 11, 2014 from http://www.datacenterknowledge.com/archives/2013/12/04/activists-target-water-supply-nsa-data-center/

Miller, R. (2014) *NSA Will Cool its Secret Servers with Waste Water*. Data Center Knowledge. Retrieved August 11, 2014 from http://www.datacenterknowledge.com/archives/2014/01/06/nsa-will-cool-secret-servers-waste-water/

Miller, R. (2014 A) *NIMBY and the Data Center: Lessons From the Battle of Newark*. Data Center Knowledge. Retrieved August 11, 2014 from
http://www.datacenterknowledge.com/archives/2014/07/22/lessons-of-the-newark-data-center-cogeneration-project-fiasco/

Miller, R. (2014 B) *Microsoft to Slash its Water Impact in Quincy*. Data Center Knowledge. Retrieved August 11, 2014 from http://www.datacenterknowledge.com/archives/2011/10/13/microsoft-to-slash-its-water-impact-in-quincy/

Ofcom. (2011). *Climate Change Adaptation: Impact on our functions. A Response to the Secretary of state's Direction of 31 March 2010*. London: Author. Retrieved August 5, 2014 from
http://www.ofcom.org.uk/binaries/consultations/ofcomresponses/Climate-change-adaptation.pdf

Ospina, A.V., Faulkner, D., Dickerson, K. & Bueti, C. (2014) *Resilient Pathways: the adaptation of the ICT sector to climate change*. Geneva: International Telecommunication Union (ITU).
http://www.itu.int/en/ITU-T/climatechange/Documents/Publications/Resilient_Pathways-E.PDF

PBS Newshour. (October 28, 2013). New York uses lessons learned from Sandy to build defenses against super-storms. Retrieved August 11, 2014 from: http://www.pbs.org/newshour/bb/science-july-dec13-sandy_10-28/

Quanta Technology. (2009) *Cost-Benefit Analysis of the Deployment of Utility Infrastructure Upgrades and Storm Hardening Programs*. Retrieved August 8, 2014 from http://www.puc.texas.gov/industry/electric/reports/infra/utlity_infrastructure_upgrades_rpt.pdf

Ricardo AEA. (2014) *Climate Change Agreement for data centers – a recognition of the sector's contribution*. Retrieved August 5, 2014 from http://www.ricardo-Horrocks et al..com/cms/climate-change-agreement-for-data-centers-a-recognition-of-the-sector-s-contribution-2/#.U9t7kONdV1E

SEC (2010) *Commission Guidance Regarding Disclosure Related to Climate Change* Securities and Exchange Commission. 17 Cfr Parts 211, 231 and 241 from http://www.sec.gov/rules/interp/2010/33-9106.pdf

SourcingFocus (2014) *Cloud promoted as a tool to combat weather disruption.* Retrieved August 11, 2014 from http://www.sourcingfocus.com/site/newsitem/8051/

Stevenson, R. (2014) *An Inconvenient (Data Center) Truth*. Data Center Knowledge. Retrieved August 5, 2014 from http://www.datacenterknowledge.com/archives/2014/03/13/inconvenient-data-center-truth/

Svenson, P. (November 15, 2012) *Verizon and AT&T: After Hurricane Sandy, Wireless Networks At 100 Percent*. Huffington Post. Retrieved August 5, 2014 from http://www.huffingtonpost.com/2012/11/14/verizon-hurricane-sandy-service_n_2133530.html

Sverdlik, Y. (2014). Apple Data Center Energy Use Grows but Remains 100 Percent Renewable . Data Center Knowledge. Retrieved 5 August, 2014 from http://www.datacenterknowledge.com/archives/2014/07/17/apple-data-center-energy-use-grows-remains-100-percent-renewable/

The World Bank. (2012) *Thai Flood 2011: Rapid Assessment for Resilient Recovery and Reconstruction Planning*. Retrieved 11 August, 2014 from http://www.gfdrr.org/sites/gfdrr.org/files/publication/Thai_Flood_2011_2.pdf

Tschundi, W. (2013) *Guideline for Water and Energy Considerations During Federal Data Center Consolidations*. US Department of Energy's Federal Energy Management Program. Retrieved August 5, 2014 from http://energy.gov/sites/prod/files/2013/12/f6/consolidation_guidelines.pdf

UK Climate Impacts Programme (UKCIP) 2013, *Ofcom's fixed asset market review – overview of climate change impacts*. Oxford: UKCIP from http://stakeholders.ofcom.org.uk/binaries/consultations/fixed-access-market-reviews/responses/Openreach_-_UKCIP_report.pdf

Uptime Institute. (2010) *Natural Disaster Risk Profiles for Data Centers*. Retrieved 30 June, 2014 from http://uptimeinstitute.com/publications

URS 2010, *Adapting Energy, Transport and Water Infrastructure to the Long-term Impacts of Climate Change*, UK cross-departmental Infrastructure and Adaptation project, contract no. RMP/5456 from http://archive.defra.gov.uk/environment/climate/documents/infrastructure-full-report.pdf

US Census. (2014) *North American Industry Classification System*. Retrieved 5 August, 2014 from https://www.census.gov/eos/www/naics/index.html

Verge, J. (2014) *ROOT Shaking Up Montreal Colocation Prices*. Data Center Knowledge. http://www.datacenterknowledge.com/archives/2014/05/23/root-shaking-montreal-colocation-prices/

Verizon. (2011) Chapter 3: The US Market, Industry Overview. Retrieved August 8, 2014 from http://www.verizon.com/investor/industryoverview.htm

Verizon. (2013) *Sustainability and the Environment in 2013*, Verizon. Retrieved August 5, 2014 from http://responsibility.verizon.com/sustainability/2013#energy-reduction

Victoria Government. (2006) *Climate Change and Infrastructure: Planning Ahead.* Retrieved 14 June, 2014 from http://www.climatechange.vic.gov.au/__data/assets/pdf_file/0018/73242/ClimateChangeandInfrastructureSummary.pdf

Willows, R.I. and Connell, R.K. (Eds.). (2003) *Climate adaptation: Risk, uncertainty and decision-making*. UKCIP Technical Report. UKCIP, Oxford from http://www.ukcip.org.uk/wordpress/wp-content/PDFs/UKCIP-Risk-framework.pdf

Wong, J., & Schuchard, R. 2011*, Adapting to Climate Change: A Guide for the ICT Industry*. Business for Social Responsibility (BSR) from http://www.bsr.org/reports/BSR_Climate_Change_Adaptation_ICT.pdf

7. Annex: Mapping supply chains with input/output tables

A complementary method for accounting for the flow of goods and services through supply chains is with Use Tables. These data, collected by the US Bureau of Economic Analysis (BEA), account for the flow of value between sectors, as well as within sectors, by tabulating the value of inputs to an industry. For this project, we initially intended to map value flows between sectors using these data, quantifying what these sectors purchase as a starting point. However, some limitations, discussed below, limited their usefulness in this report.

The two figures below illustrate the top ten sectors by producer values that provide inputs to the telecommunications and data centers sectors.

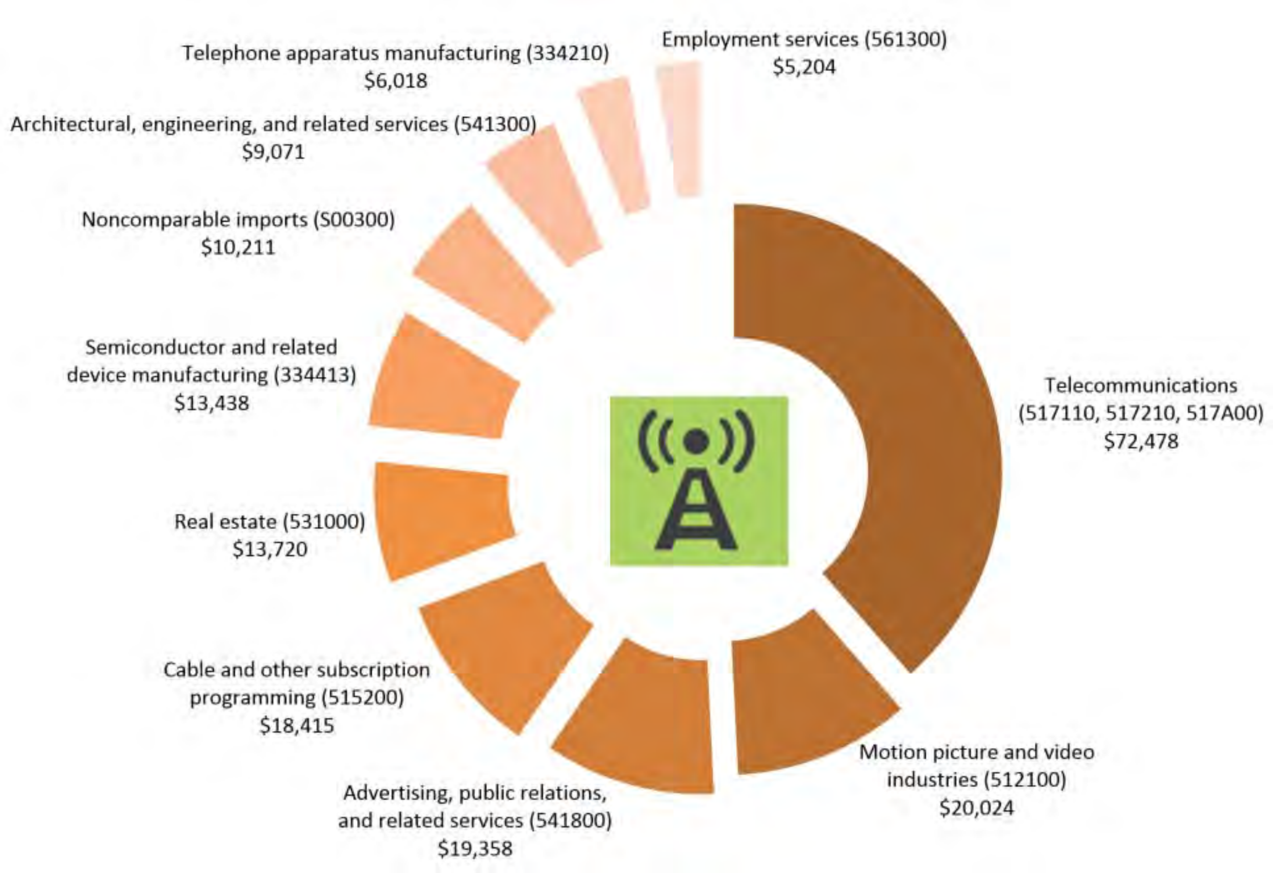


Figure 6 - Top ten industry and commodity inputs (millions of USD, adjusted for inflation to 2014 values) to the US telecommunications sector (combined NAICS codes 517110, 517210, 517A00) (BEA, 2007)

The NAICS 2007 codes are used in this analysis (in place of the newer 2012 codes) since they provide input/output measures for more sectors. However, in
Figure 6, three 2007 NAICS codes that encompass telecommunications as defined in the latest code for telecommunications (517) were combined. These three 2007 codes for telecommunications are:

- Wired telecommunications carriers (2007 NAICS code 517110)
- Wireless telecommunications carriers (except satellite) (2007 NAICS code 517210)
- Satellite, telecommunications resellers, and all other telecommunications (2007 NAICS code 517410)

The largest input to the telecommunications sector is intra-sectoral. This is due in part to the combination of the three telecommunications subsectors, but also reflects the prevalence of shared infrastructure and services between telecom providers, the importance of manufacturers, non-comparable imports[3], and real estate reflect the supply chain maps above. This internal trade may also reflect indirect use of electricity and water services supporting critical shared infrastructure. However, the high value attributed to inputs from “Motion picture and video industries” and “Advertising, public relations...” industries is counter-intuitive and, as neither sector is likely to be a source of climate risk, these are not reflected in the supply chain maps above.

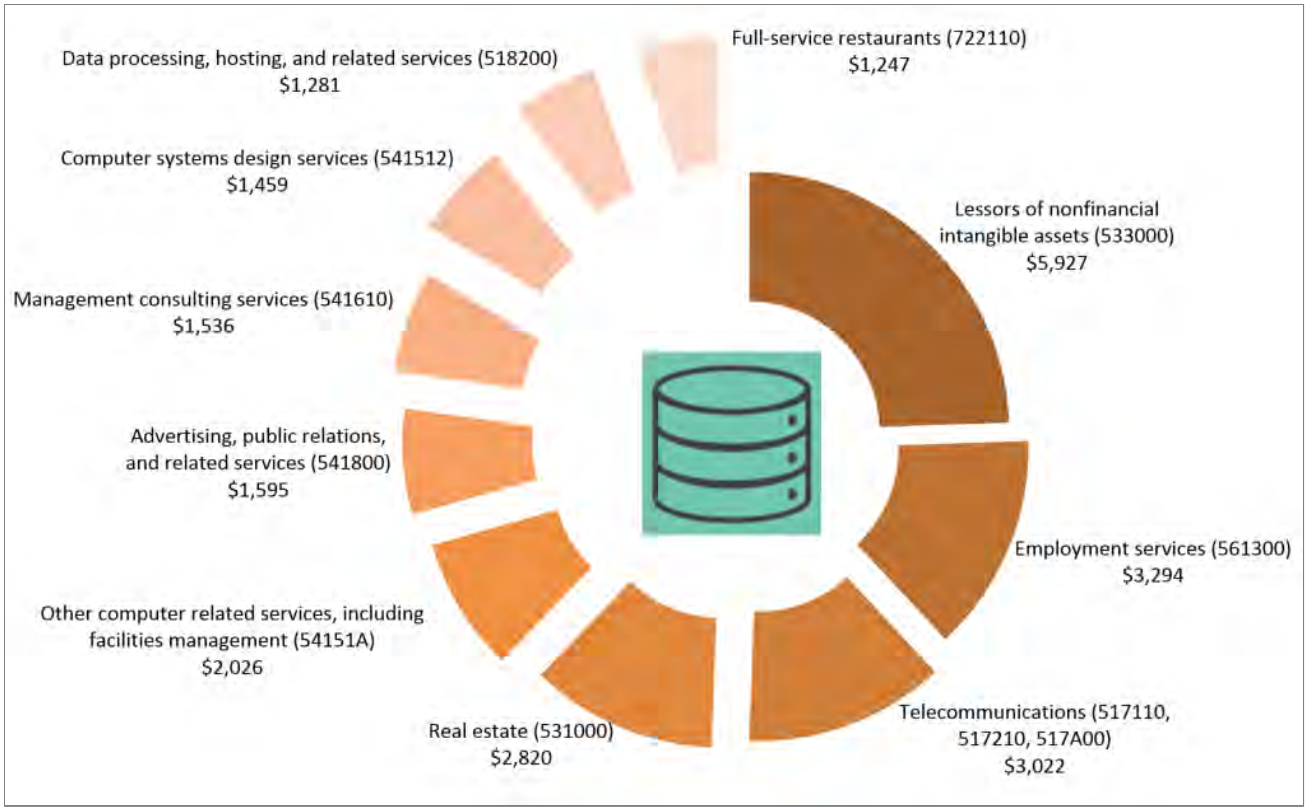


Figure 7 - Top ten industry and commodity inputs (millions of USD, adjusted for inflation to 2014 values) to the US data center services sector (BEA, 2007)

Figure 7 shows the inputs to the data center services sector. The largest input industry to data centers is “lessors of nonfinancial intangible assets,” which encompasses companies that own and assign rights to patents. This and employment services, the second largest input, are not intuitively faced with climate risk, and thus also do not feature in the supply chain maps despite their significance to the sector. The appearance of telecommunications, real estate, computing services, and other related industries reinforces the supply chain maps, demonstrating the importance of those industries where physical assets and siting issues suggest a greater likelihood of climate risk.

There are some clear limitations to using input/output tables for understanding climate risk to telecoms and data centers. For example, critical inputs known to be at high climate risk, such as electricity, do not rank as high value inputs, despite the fact that power sources are critical to both sectors and an area

[3] Incomparable goods are defined as goods bought abroad that do not have domestic equivalent.

where climate risk should be assessed. Likewise, low levels of financial expenditures in a sector are not emphasized in these figures, but small dollar values do not necessarily correlate with low climate risk. Also, supply chains can contain many non-tangible elements, such as patents, that feature prominently in Use Tables but are unlikely to be affected by climate change. The supply chain maps presented in the report reflect the essential inputs that can be affected by climate change, and are thus better tools for conceptualizing and ultimately addressing risk and identifying opportunities in a changing climate.