



Adapting the ICT Sector to the Impacts of Climate Change Summary Report

Crown Copyright
ED49926
Issue 2
September 2010


Title	Adapting the ICT Sector to the Impacts of Climate Change – Summary Report
Customer	Defra
Customer reference	RMP 5604
Confidentiality, copyright and reproduction	<p>Crown Copyright</p> <p>This report is Crown Copyright and has been prepared by AEA Technology plc under contract RMP 5604 to Defra dated 2 March 2010. The contents of this report may not be reproduced in whole or in part, nor passed to any organisation or person without the specific prior written permission of Defra. AEA Technology plc accepts not liability whatsoever to any third party for any loss or damage arising from any interpretation or use of the information contained in this report, or reliance on any views expressed therein.</p>
File reference	ED49926
Reference number	ED49926 - Issue 2

AEA group
329 Harwell
Didcot
Oxfordshire
OX11 0QJ

t: 0870 190 3862
f: 0870 190 6318

AEA is a business name of AEA Technology plc

AEA is certificated to ISO9001 and ISO14001

Author	Name	Lisa Horrocks, John Beckford, Nikki Hodgson
Approved by	Name	Geoff Dollard
	Signature	
	Date	22 September 2010

Disclaimer

Adapting the ICT Sector to the Impacts of Climate Change – Summary Report

This is an independent report commissioned by the cross-departmental *Infrastructure and Adaptation* project.

Its findings, conclusions and recommendations are not endorsed by Government but will be considered by the project as part of its two-year programme of work to identify and examine strategic solutions to improve the long-term resilience of new and existing infrastructure in the energy, ICT, transport and water sectors to future climate change impacts.

Acknowledgements

This report was written by AEA, supported by Beckford Consulting. Many people have been engaged in discussion with the project team, either at the expert workshops or informally during the course of the study. We would like to express our thanks and acknowledge the useful contributions that each has made to the study. We are also grateful to those officials within Government who commented on the draft of the full Final Report.

Citation

This report should be cited as:

Horrocks, L, Beckford, J, and Hodgson, N. (2010). Adapting the ICT Sector to the Impacts of Climate Change – Summary Report, Defra contract number RMP5604. AEA group, published by Defra.

Executive summary

The UK is reliant on a set of critical infrastructures for, among other things, water, energy, transport and communications to enable much of what we do every day.

This report summarises the findings of a scoping study to explore the impacts of climate change on the ICT sector and the potential for adaptation.

This study has found that:

- **To some extent, the ICT sector is inherently resilient and adaptable to climate impacts, although this is not necessarily the case at the level of an individual end-user.**
- **Providers and consumers of ICT will nevertheless need to consider adaptation, because of the UK's increasing dependence on ICT and increases in extreme weather events.**
- **ICT is vulnerable to a number of current and future climate risks, in the UK and internationally.**
- **Climate impacts on ICT can have considerable cross-sectoral implications for infrastructure and business.**
- **Adaptation options for the ICT sector will enhance the resilience of the infrastructure, take advantage of new technologies and improve business processes.**
- **There will be an important role for ICT infrastructure providers and ICT consumers, alongside government, in overcoming the barriers to adaptation.**

Table of contents

1	Introduction	1
1.1	Project Context	1
1.2	Approach	2
2	The ICT sector in the UK	3
2.1	Definition of ICT	3
2.2	Role of ICT	4
2.3	Resilience in the ICT sector	5
2.4	Lifetimes of ICT infrastructure components	5
3	Climate impacts on ICT	7
3.1	UK climate risks to the sector	7
3.2	International climate risks to the sector	10
4	Consequences of climate impacts	13
5	Cross-sectoral and business implications	15
6	Adaptation in the ICT sector	17
6.1	Adaptation for ICT	17
6.2	Challenges and barriers	19
7	Conclusions and Recommendations	21
7.1	Conclusions	21
7.2	Recommendations	24

1 Introduction

The UK is reliant on a set of critical infrastructures for, among other things, water, energy, transport and communications to enable much of what we do every day. Against the background of a growing programme for adapting to climate change across the public sector, UK Government is also considering how to improve the long-term resilience of new and existing infrastructure to future climate change impacts.

This report summarises the findings of a scoping study to explore the impacts of climate change on the ICT sector and the potential for adaptation.

For full details of the study, please refer to the full Final Report.

Climate change in the UK is predicted to bring increases in average temperatures and further sea-level rise, increasing frequency and intensity of extreme weather events (e.g. intense rainfall, very hot temperatures) with potential for droughts, increased flooding, heatwaves and greater pressure on resource availability, particularly water.

National infrastructure will be affected by these impacts and given the dependence upon multinational organizations, international markets and global supply chains, the UK ICT sector is also potentially at risk from the impacts of climate change occurring elsewhere in the world. This is recognised in the cross-Government Adapting to Climate Change (ACC) Programme which has prioritised adapting national infrastructure while the Council for Science and Technology¹ recognised that resilience against climate change is the most significant and complex longer-term challenge facing our national infrastructure.

The Climate Change Act (2008) created a framework for building the UK's ability to adapt to climate change. The Act includes a power for the Secretary of State to require 'bodies with functions of a public nature' and 'statutory undertakers' to report on how they have assessed the risks of climate change to their functions, and what they are doing to address these risks (the Adaptation Reporting Power). The potential vulnerability of the ICT sector to climate change risks is underlined by the fact that Ofcom has been directed to report, and that other organisations within the ICT sector will be encouraged to report voluntarily.

1.1 Project Context

This work has been undertaken as part of the ACC's cross-departmental *Infrastructure and Adaptation* Project, which aims to identify and examine strategic solutions to increase the long-term resilience of energy, ICT, transport and water infrastructure to future climate change impacts. There is as yet very little prior work which specifically considers the potential impacts of climate change on ICT, particularly in the context of current and future developments and emerging technologies, and the consequent knock-on to other parts of the infrastructure "system of systems".

Aims and objectives

The aim of the study, as required in the specification, was to:

- a) Examine the impacts of climate change on the ICT sector
- b) Examine the technical and operational impacts on the sector
- c) Examine what this means for other infrastructure sectors
- d) Examine how the sector needs to adapt to climate change
- e) Examine how far the current configuration of the sector facilitates climate change adaptation
- f) Identify:
 - i) What changes will be required to increase resilience
 - ii) What barriers need to be overcome
 - iii) Recommendations for action

¹ CST (2009) A National Infrastructure for the 21st Century <http://www.cst.gov.uk/reports/files/national-infrastructure-report.pdf>

While the scope of this study is England-only, it sits within a broader UK government context for identifying and managing risks relevant to national infrastructure. The work carried out for this study starts to address the gap in knowledge relating to climate change and its potential impacts on the ICT sector, and explores the critical interdependencies of other infrastructure sectors on ICT in the context of climate risks and building climate resilience. While we have concentrated on the impacts of climate change in the UK, we have also considered the global nature of the changing climate insofar as it impinges upon the ICT services used in the UK.

1.2 Approach

The study involved an evidence review, a workshop with experts working within the ICT sector, and follow-up research and analysis on key issues and case studies.

2 The ICT sector in the UK

ICT is already integral to the functioning of UK national infrastructure, our economy, and society, and is becoming increasingly so. ICT is an enabler of growth and change, with, for example, a growing reliance on and expectation of ICT to facilitate many aspects of the transition to a low-carbon economy.

The ICT sector is different in nature from the 'heavy' infrastructure sectors, such as energy, transport and water, in a number of ways: the infrastructure is generally smaller and has shorter lifetimes; rather than individual structures, it is the combined network which is the ICT infrastructure asset; ICT services in the UK have a strong international dimension and dependence; the sector is highly competitive in both service and infrastructure provision resulting in some inherent redundancy; and, the sector is characterised by a rapid pace of development and change with continual introduction of new technologies.

Many of these features mean that the ICT sector is to some extent both inherently resilient (in that there are multiple networks and/or ICT services available to customers) and inherently adaptable (in that short lifetime components can be updated and refined to meet changing needs).

2.1 Definition of ICT

Within this study, ICT was taken to mean "the whole of the systems and artefacts which enable the transmission, receipt, capture, storage and manipulation of voice and data traffic on and across electronic devices". As such it includes:

- all the infrastructure components of copper and fibre optic cables, exchanges, masts, aerials and antennae;
- system devices (e.g. network switches, routers, wireless access points);
- end-user devices (e.g. computers –both portable and desktop, telephones, mobile telephones, PDA and other hand-held devices, SCADA control devices, GPS transmitters/receivers)
- satellites (taken as outside the scope of this study);
- applications (e.g. the programmes that enable the infrastructure and devices to function, interact and perform useful functions);
- services integral to the provision of ICT (e.g. data centres, call centres, electronic data interchange, on-line commerce);

Provision of energy (electricity) to power ICT is outside the scope, though we recognise that this is a fundamental requirement and critical dependency for the whole sector.

Telecommunications is the assisted transmission of signals over a distance for the purpose of communication. The key telecommunications are broadband services, mobile voice and data services, fixed voice services and broadcast services. Telecommunications is included within the definition of ICT above for the purposes of this study.

ICT works as a complete system and both user and system devices are designed to conform to industry agreed standards for operating range tolerances, data receipt and transmission and ability to connect with other devices.

In this context, there are three points to consider:

1. That all of the above artefacts work together as a system – inter-connected, interdependent and completely enmeshed in each other and working to absolute rules of inter-operability. As such, the national asset is the network rather than any of the individual components.
2. That whilst the network is the asset at the level of infrastructure, the value of the network is not in the asset itself but in the information which travels on it. Nearly the whole of the economy relies upon the ability to transmit, receive and convert digital data in close to real-time.
3. That the historic complete separation of 'voice' from 'data' traffic has been lost. At the level of network transmission, for all digital systems, they are the same thing. A further emergent

complexity is the growth of ‘power over ethernet’ in which the network cable that carries data is also used to carry electricity. This represents a convergence of the ICT sector with elements of the energy system increasing their co-functionality such that either they both work or neither works.

All of the value that may be generated through most of the UK’s economic activities is dependent on the complex system described above. Its reliable operation defines the post-industrial economy. Its resilience, including to a changing climate, is critical to national well-being.

2.2 Role of ICT

Table 1 illustrates the importance of the role that ICT plays in our lives today.

Table 1 Some key statistics demonstrating the scale of the role of ICT in the UK today

ICT Sector Key Statistics	
ICT sector is extremely important to our economy and the functioning of all sectors of our society	
The technology sector generates over £35 billion of Gross Value Added and employs over 5 million people in the wider knowledge industries	
The <i>Digital Britain</i> sectors account for nearly £1 in every £10 that the whole economy produces each year	
Estimates say 84% of UK businesses are heavily dependent on their IT systems. (PwC Information and Security Survey, 2008)	
90% of our high street purchases are transacted using plastic cards which depends on wired and wireless communications to work	
£50 billion of consumer purchases and sales in Britain take place wholly online	
In transport, the phasing of street traffic lights, the operation of railway signals and points and the wireless systems that allow aircraft to take off and land safely all need communications	
Intellect estimate 4.2 million people in the UK work flexibly - the vast majority of these use broadband and other technology to work remotely	
Sources: Department for Culture, Media and Sport and Department of Business Innovation and Skills (2009) <i>Digital Britain</i> Intellect (2010) <i>General Industry Fast Facts</i> http://www.intellectuk.org/content/view/4348/377/#general	

During normal times, ICT infrastructure is typically highly reliable. However, ICT performance under stress (and human performance when the technology does fail) can be very unpredictable and it is subject to node failure in which damage or compromise of a key element (a node, router, switch or exchange) causes a service failure to multiple users.

The increasing trend towards shared infrastructures, outsourced arrangements (including off-site data centres), emergence of ‘cloud computing’ (where both the data and the application are held remotely from the user) all have great potential to drive greater business efficiency. However these advances may simultaneously represent a reduction in the resilience of the system (its ability to operate independently of other elements of the infrastructure). This is because the ability to operate locally becomes dependent on artefacts of the system which will be remote from the user, under the control (operational and legal) of other parties, and which could generate potential single points of failure.

New generations of infrastructure are increasingly reliant for operation on a complex web of above and sub-ground connectivity. This will continue to increase the workload placed on ICT infrastructure, which in turn relies on the availability of energy for operation.

The complicated ownership pattern of the UK’s National Infrastructure (NI) in general has been highlighted by the Council for Science and Technology (CST, 2009). Most of the NI is owned, operated, built and maintained by the private sector, and is embedded in a regulatory framework, within a wider Government context. However, some sectors of the NI are more market-led than others. For example, communications are driven by consumer demand for the latest technology resulting in the rapid expansion of mobile phone usage and home computing.

2.3 Resilience in the ICT sector

The concept of **resilience** is used in many contexts. In the Government's Critical Infrastructure Resilience Programme², resilience is defined as “the ability of a system or organisation to withstand and recover from adversity”.

In the context of climate impacts, the UK Climate Impacts Programme³ defines resilience as “the ability of a social or natural system to absorb disturbances while retaining the same basic structure and ways of functioning, the capacity of self-organisation and the capacity to adapt to stress and change”.

For the purposes of this study, we restricted ourselves to a consideration of *building resilience to climate impacts*, recognising that climate resilience is just one aspect of overall resilience needed within the ICT sector.

We use the term “adaptation” to refer to the actions which can be taken to enhance resilience to climate impacts: these actions might be undertaken by government, by organisations providing ICT infrastructure or services, or by wider stakeholders in the ICT sector, namely all of the organisations and individuals who rely upon ICT for business, commerce or leisure.

It is in the interest of ICT providers, in an extremely competitive market, to maintain service by ensuring a good level of resilience. The Cabinet Office⁴ considers that resilience of national infrastructure in the telecommunications sector is conferred by:

- The ability to switch between the major networks in the event of failure;
- The competitive nature of the market, which should encourage building resilience within business models;
- The ongoing co-operation between Government and the sector through a number of fora;
- The ongoing programme of work to ensure essential lines of communication (e.g. for the emergency services) are maintained in the event of the failure of the network.

For the purposes of this study, we highlight that while *from the perspective of maintaining critical communications* at a national level, the sector is to an extent inherently resilient to current and future climate impacts, *from the perspective of the consumer*, what actually matters is the loss of an essential service, irrespective of whether it arises from the loss of assets or services deemed “critical” at the national (or even regional or local) level.

It is worth noting the distinction between publicly-provided infrastructure, such as cable infrastructure, and privately-owned ICT, such as dedicated data centres. The responsibility for ensuring that there is sufficient provision of ICT to meet users’ needs (in the face of a whole range of current and future challenges, including climate change), rests with both the customer / end-user, and the public infrastructure provider, to greater or lesser extents, depending upon the particular context.

2.4 Lifetimes of ICT infrastructure components

The ICT sector is renowned for the rapid pace of development and technological change. As a consequence it has a high rate of infrastructure renewal for devices contrasting with a much lower refresh rate for the buildings and masts which accommodate those devices.

Figure 1 illustrates the relative lifetimes of various components in the ICT sector, alongside approximate timeframes for climate change. This shows that, unlike other national infrastructure sectors, the majority of the components that make up ICT may be renewed and replaced many times before the major effects of climate change will be felt.

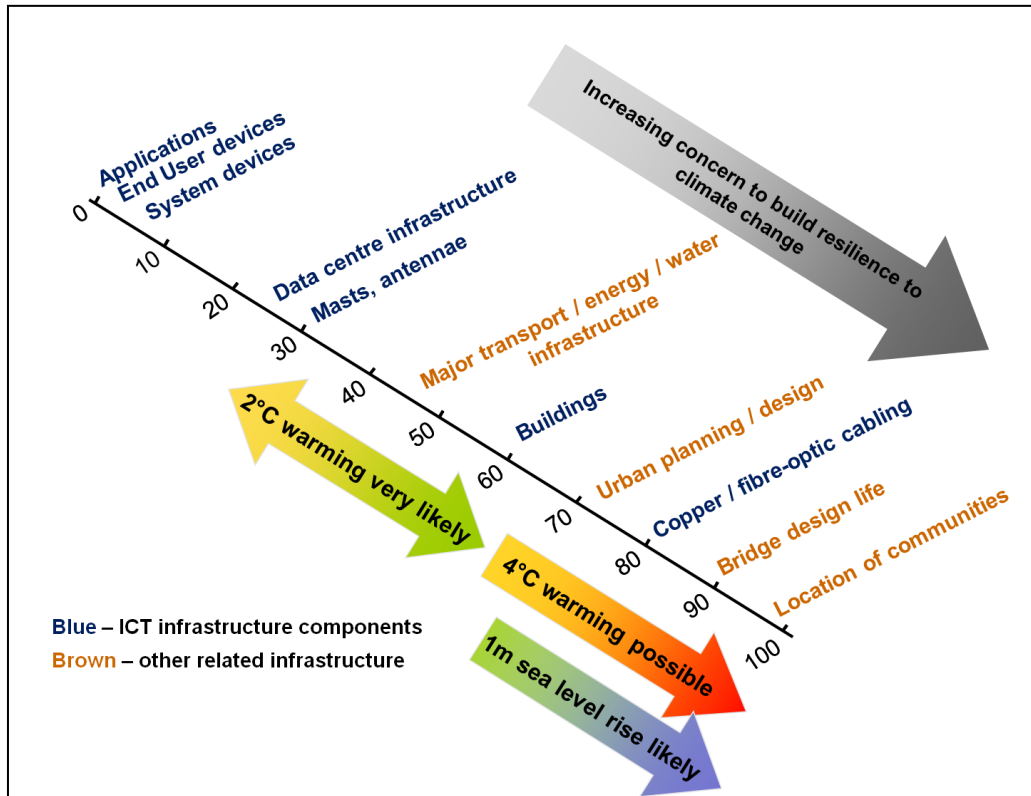
² Cabinet Office (2010) Strategic Framework and Policy Statement
www.cabinetoffice.gov.uk/ukresilience/infrastructure/resilience.apsx

³ Definition available from online Glossary at www.ukcip.org.uk, visited on 28/03/2010

⁴ Cabinet Office (2010) Sector resilience plan for critical infrastructure
www.cabinetoffice.gov.uk/ukresilience/infrastructure/resilience.apsx

Gradual trends in climate are unlikely to have a significant effect, because there is scope for new technologies to develop and adapt with every refresh cycle. To some extent, the pace of technology change, and the high refresh rates give the sector a high capacity to adapt in a flexible and almost reactive manner to climate change, provided that the evolving risks over coming decades are factored into design decisions. The longer-lived assets (buildings used for various purposes, mast structures, and copper (or fibre-optic) cabling) may feel the effect of gradual trends. In all cases, it is the extremes of weather that already present the greatest challenge to resilience.

Figure 1 Lifetimes (in years) of ICT infrastructure components compared with climate change



3 Climate impacts on ICT

Weather already has the potential to interrupt, or reduce the quality of, ICT services, through a wide range of direct and indirect impacts, including international impacts on supply chains. Extreme weather leading to floods or heatwaves is a particular concern. The changing climate is expected to bring increases in this kind of weather, in both frequency and severity.

Climate risks will become an increasing concern for the ICT sector, because of the combination of (a) increasing dependence upon ICT and demand for high quality, uninterrupted, reliable service provision in all areas of business, commerce and leisure, and (b) increasing frequency and severity of the kinds of weather events which can already cause disruption in the sector.

3.1 UK climate risks to the sector

The majority of devices typically used in the UK already have operating tolerances to temperature and humidity which will accommodate UKCP09 predicted temperature changes, provided they are appropriately installed and maintained.

While the topic has been little-studied to date, there is a wide range of current vulnerabilities to weather impacts within the ICT sector, and therefore the potential for some significant impacts from climate change. Weather has the potential to interrupt, or reduce quality of, ICT services. The Climate Projections indicate that over the coming decades, the frequency and severity of extreme weather events is likely to increase. These evolving risks will need to be considered as devices are replaced and upgraded.

- Those elements of the infrastructure which are below ground are vulnerable to flooding, rising water tables, water ingress (particularly during times of snow melt or flooding), subsidence caused by drought or flooding, and consequential risks arising from damage to other elements of the infrastructure. For example, bridge failure during floods at Cockermouth in 2009 also damaged telephone and power transmission lines.
- Above ground, the infrastructure (masts, antennae, switch boxes, aerials, overhead wires and cables) are at risk from precipitation (water ingress, snow melt), wind, snow (weight), unstable ground conditions (flooding, subsidence) and changes in humidity. High humidity can lead to condensation with risk of short-circuiting of equipment. There is also risk to the serviceable lifespan of the artefacts brought about by increased environmental stress (high winds, greater temperatures).

Table 2 summarises the main potential climate impacts on ICT identified during this study. The table also shows the consequences of these climate impacts, and the level at which the impact might be felt, from an individual organisation, to a local area, or across the national network.

There is a distinction between public ICT, such as cable infrastructure, and privately-owned ICT, such as dedicated data centres. The responsibility for addressing climate impacts will therefore in some cases fall to the customer or end-user, rather than the public infrastructure provider.

Table 2 Potential climate impacts on ICT and their consequences and level of impact. (Red crosses indicate a potential negative effect, green ticks a potential positive effect, and black bi-directional arrows where the direction of the effect is uncertain.)

Climate impacts on ICT		Potential Consequences						Level of impact		
Climate factor	Potential impact	Degradation of infrastructure	Availability of services	Quality of services	Repair and recovery	Business costs	Health and safety	National	Local	Individual (organisation)
Increase in daily maximum temperatures (and higher frequency of “very hot” days and heatwaves in summer)	Increased risk of overheating in data centres, exchanges, base stations, etc (increased air-conditioning requirements and costs, failure of free-air cooling)		×			×	×		●	●
	Increased heat-related health and safety risks to exposed workers (e.g., maintenance engineers, drivers, staff in exchanges)				×		×			●
Increase in average temperatures	Location / density of wireless masts may become sub-optimal since wireless transmission is dependent upon temperature (refractive index)		×	×		×			●	●
	Impact on quality of radio-frequency propagation if vegetation type changes in response to climate			×					●	
Increase in minimum temperatures (fewer frost days and less snowfall)	Reduced costs of space heating in assets (data centres, exchanges, etc) in winter					✓				●
	Reduced impacts of snowfall on masts, antennae, etc, requiring less maintenance	✓	✓			✓	✓	●		
	Less frequent requirement to cope with snow-melt water surge (flood) problems	✓	✓		✓	✓	✓		●	●
Increase in extreme daily precipitation in winter (and higher frequency of “very wet days”)	Increased risk of flooding of low-lying infrastructure, access-holes and underground facilities	×	×			×	×		●	
	Increased erosion or flood damage to transport structures which may expose cables / trunk routes	×	×			×			●	●
	Reduced quality of wireless service with higher rainfall rates			×				●		

Climate impacts on ICT		Potential Consequences						Level of impact		
Climate factor	Potential impact	Degradation of infrastructure	Availability of services	Quality of services	Repair and recovery	Business costs	Health and safety	National	Local	Individual (organisation)
	Increased flood risk to assets located in flood plains or urban environments (increase in flash floods), e.g. data centres, exchanges		✗		✗	✗			●	●
	Increasing difficulty to repair faults and restore service with increasing volume of adverse weather-related problems		✗	✗	✗	✗	✗		●	●
Decrease in daily precipitation in summer (and greater likelihood of drought)	Increased risk of subsidence, reduced stability of foundations and tower structures	✗				✗			●	
Changes in storminess and wind	Changes in storm / wind-loading damage to all above ground transmission infrastructure	↔	↔		↔	↔			●	●
	Lightning strike damage to transmitters	↔	↔	↔		↔			●	●
Rising sea levels (particularly in south-east and eastern England) and increase in storm surges	Increased saline corrosion of coastal infrastructure (broadcasting towers, etc	✗				✗			●	
	Increased risk of coastal erosion and coastal flooding of infrastructure (e.g. exchanges) in vulnerable areas	✗	✗		✗	✗	✗		●	●
	Potential change in reference datum for some telecommunication / satellite transmission calculations			✗					●	
Changes in (absolute) humidity	Changes in corrosion rates	↔				↔		●		
	Changes in requirements for dehumidification to maintain internal environments within tolerance ranges of system devices					✓				●

Buildings

The ICT sector, as any other, will need to deal with the general range of climate risks to the built environment, managing a heritage of built assets which were not designed (or located) with any consideration of climate change. An additional challenge for ICT is that the sector is already managing buildings that were not optimally designed for their current purposes. For example, the Northern Rail Data Centre at Newton Heath, Manchester, is housed in an old Railway Engineering Depot; many mobile telecommunications masts are mounted on long-established buildings (such as churches); many of BT's exchanges are still in original Victorian buildings.

Data Centres

There is ongoing growth in the number of data centres, outsourced services, call-centres and, most recently the emergence of 'cloud computing', in which both data and applications are run across the internet, remote from the user. All these developments mean that operations rely absolutely on the availability of power and continuous data connectivity. This imparts significant vulnerability to the whole ICT system, primarily connected with the physical location of the data centres and call centres, which have the same vulnerability to climate change as any other above ground structure.

The economic and social impact of the failure of a data centre is potentially very high given the role they play in enabling the economy to function. The siting of future data centres needs to take climate change risk into account in relation to both the centre itself and its power supply, and they must be designed to be systemically resilient, i.e. resilient in the context of the whole network asset, not simply in isolation from the other artefacts.

Wireless transmission

Wireless continues to grow as an applied technology offering advantages in speed and cost of deployment, though currently not providing data transmission speeds equivalent to wired connections. Wireless can be affected by climate change in different ways.

1. Temperature increases impact the range over which wireless signals can be sent and received. Rising extreme temperatures will impact range.
2. Precipitation (rate of rainfall and size of raindrop) adversely affects quality of service (the reliability of the wireless receivers at capturing complete transmissions).
3. The physical environment, e.g. density of foliage, the shape and construction methods of buildings, all have a significant impact. As buildings are developed and adapted to cope with the demands of climate change it will be necessary to ensure that wireless transmission continues to be possible. It is already the case that metal foils used in the structure of modern buildings as part of insulation are inhibiting mobile phone signals.

Seasonality

Most climate impacts are seasonal in nature. This can mean that climate change brings negative impacts in summer, but some positive effects in winter (or vice versa). An example would be the greater challenge of dealing with more very hot days during summer, but an anticipated reduction in the extent of cold winter maintenance. However, because of climate variability, it is important to recognize that occasional cold weather extremes are expected to occur, albeit with less frequency. This may make it more difficult for telecommunications providers to respond to the cold weather impacts when they do occur, since the relevant skills and experience of similar events may diminish over time.

3.2 International climate risks to the sector

The extent to which the ICT sector is internationally interdependent is probably unique. This interdependence extends not just to the provision of materials and devices but also to the hosting, storage and transmission of the data itself. There is therefore a risk from climate impacts all over the world for the ICT sector, rooted in dependence upon international connectivity.

Considering this from a supply chain perspective, much of the physical infrastructure is internationally sourced, ranging from pine telegraph poles to rare and precious metals. Assuming availability, the international shipment of components and materials (including completed products) is threatened if climate change leads to severe weather events that disrupt air and sea carriage.

Rising sea levels and extreme weather events could also affect the operation of data centres and service centres in low lying areas such as the Netherlands and vulnerable areas of the sub-continent of India. The full risk associated with 'off-shoring' of data, service and call centres needs to be evaluated but is beyond the scope of this work.

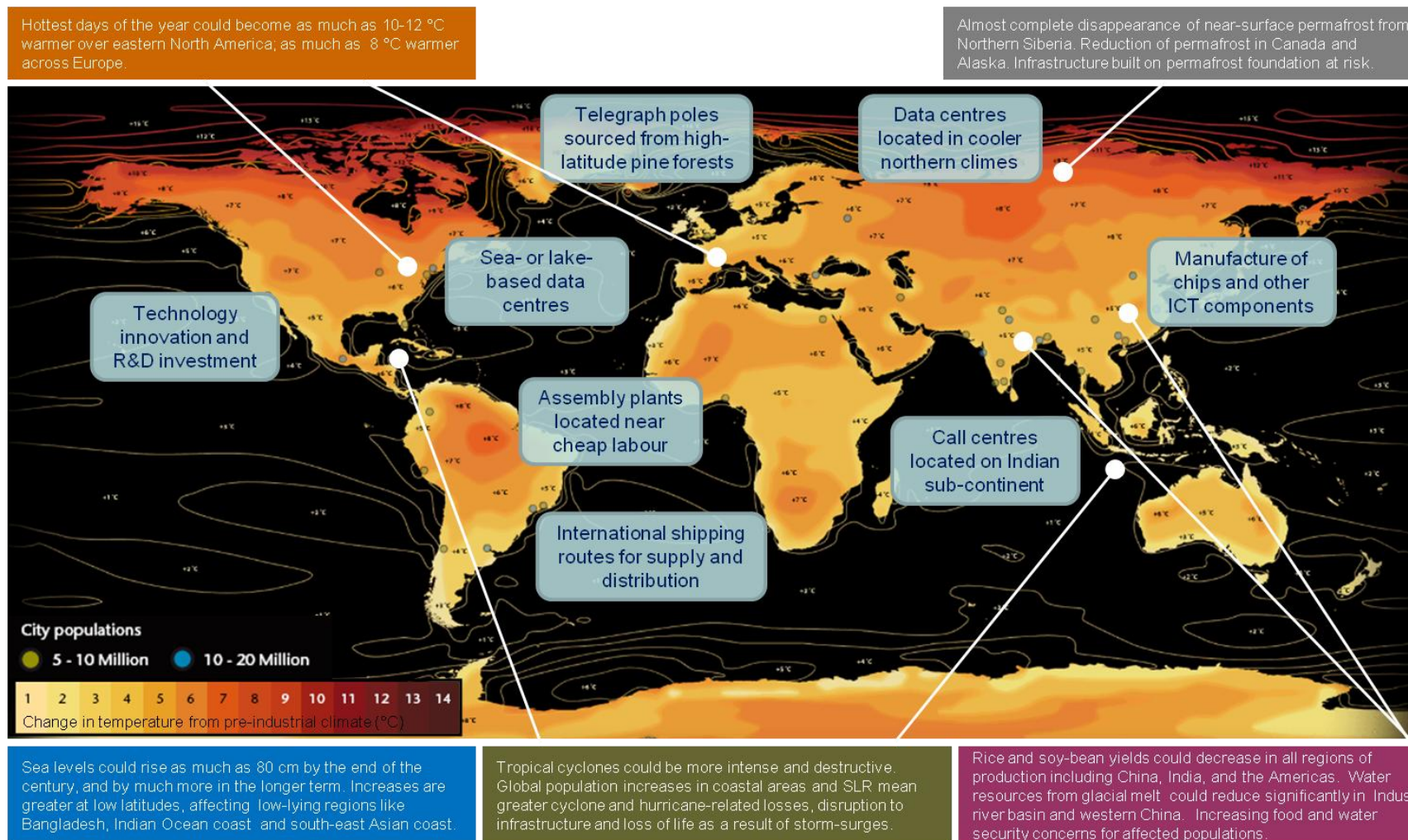
Both within the UK and internationally, increasing incidence of extreme weather events could prevent employees reaching either their normal place of work or attending sites to repair or restore failed components of the infrastructure (base stations, antennae, exchanges). These weather events are also likely to generate increased use (transmission volumes) of the ICT infrastructure as greater numbers work at a distance from their normal place of work. Increased demand places greater dependence on the reliability and resilience of the ICT network.

Increasing use of wireless technologies means competition for those parts of the spectrum which have greatest environmental resilience. Radio spectrum could become a tradeable commodity at the international level, impacting availability, cost and resilience.

Long-term resilience in ICT will draw upon investment in research and development. Reflecting the sources of both intellectual property and physical devices, the UK should probably be considered vulnerable due to its relative position as a buyer rather than a supplier of these elements.

Figure 2 illustrates some of the ways in which climate change around the world may affect ICT in the UK.

Figure 2 Potential international climate impacts on the ICT sector. Underlying chart illustrates temperatures changes for a 4°C global average warming (from www.decc.gov.uk)



4 Consequences of climate impacts

There is a wide range of ways in which climate change may impact upon ICT infrastructure and service provision, linked to increasing temperatures (particularly heatwaves), more extreme rainfall leading to flooding, and sea level rise. The consequences of these impacts, alone or in combination, are:

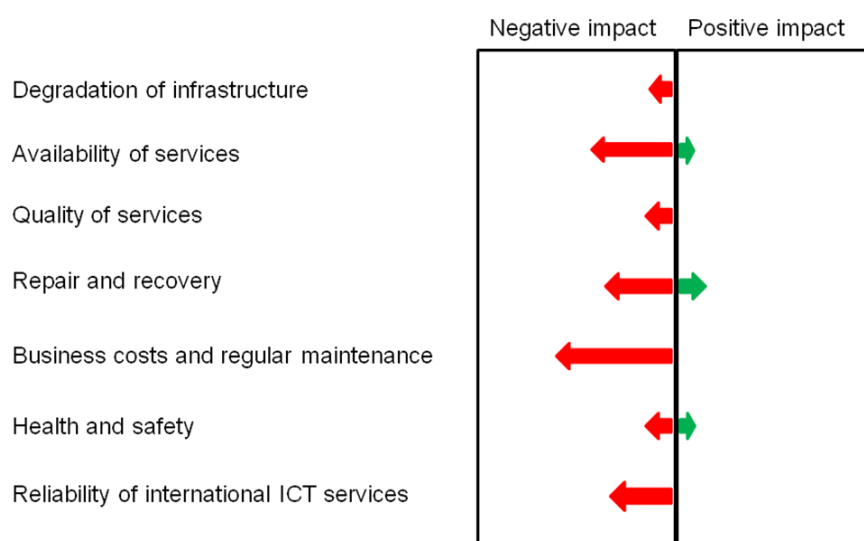
- environmental degradation of infrastructure, leading to changes to the expected in-service lifetime of longer-lived structures (such as mobile transmission masts);
- changes to the availability or reliability of ICT services, from disruption caused directly or indirectly by weather events; changes to the quality of service provision, particularly connected to the dependence of wireless signal quality on environmental factors;
- implications for repair and recovery following extreme weather damage or disruption in any aspect of the infrastructure, potentially resulting in additional costs;
- changes to operational business costs, such as heating and air conditioning requirements;
- changes to working environments and associated health and safety of employees; and,
- changes to the reliability of international ICT services.

While climate change looks to bring predominantly negative impacts and increasing costs, there are some positive opportunities.

Very few impacts are expected to affect the entire national ICT network. The majority of impacts are likely to cause disruption at the level of individual organisations or local geographical areas as a result of small parts of the telecommunications network being affected by localised weather events. More worryingly is the potential knock-on of even some localised disruption to ICT services on interdependent infrastructure and business sectors.

Climate change may impact on the ICT sector in a wide variety of ways, with consequences which may be negative (for example leading to higher costs) or positive (for example, savings from reduced maintenance). These positive and negative effects are illustrated in Figure 3.

Figure 3 Relative consequences arising from climate change impacts on the ICT sector



While climate change looks to bring predominantly negative impacts and increasing costs, there are some positive opportunities. Many of these are linked to the projected increase in winter temperatures, and potentially a reduction in damage to infrastructure (snow-loading) and disruption to maintenance and repair schedules. Additionally, engineers could be less frequently exposed to the potential safety issues of working in icy conditions.

More widely, climate change may present some indirect business opportunities for the sector. For example, globally, there is an increasing demand for early warning systems and associated environmental sensors and communications to improve management of extreme weather hazards. The ICT sector will be instrumental in enabling these developments. The ICT sector is pioneering in relation to some aspects of security and risk management (notably information and cyber security). There may be an opportunity for some of this expertise in security and resilience to be refocused onto the issue of climate change, such that the sector provides leadership and innovative solutions for other sectors and organisations addressing climate risks.

Very few impacts are expected to affect the entire national ICT network, and those that do are related to probably minor changes in quality of signal resulting from temperature effects on radio-frequency transmission. Thus it is accurate to say that from a national, strategic perspective, climate change does not look to pose a significant threat to the resilience of the national network as a whole.

However, that is not to say that the risk is insignificant. The majority of impacts are likely to cause disruption at the level of individual organisations or local geographical areas, e.g. as a result of small parts of the telecommunications network being affected by localised weather events. Rural locations, those at the end of a network line, or served by only one or two networks are most vulnerable to disruption. From the perspective of individual businesses, therefore, climate change may pose some additional challenge to the continuation of “business as usual”. In addition, it is also possible for localised incidents to have a considerable impact, as was experienced when a major flood at a BT exchange in Paddington, London, affected broadband and telephone services across the UK, in March 2010⁵.

⁵ While this particular flood was not reported to have a weather-related cause, the consequences illustrate the potential consequences of flooding from any cause. See, for example, BBC news coverage of the event at <http://news.bbc.co.uk/1/hi/technology/8597399.stm>

5 Cross-sectoral and business implications

While the ICT sector is dependent upon the provision of energy, all other sectors are dependent upon ICT. Resilience in the ICT sector is critical to the continued operation of the other national infrastructure sectors, and business in general.

Direct climate impacts which cause disruption of ICT services can lead to a very wide range of indirect implications in other sectors. To a lesser extent, direct climate impacts elsewhere can have secondary effects on the ICT sector, for example, climate change affecting consumer and business trends, climate change affecting energy security and water availability, weather damage to other structures affecting fixed cables.

A recent report⁶ on the systemic interactions of UK national infrastructure stated that the five sectors (energy, ICT, transport, waste and water) were to some extent all interdependent, but that each was absolutely dependent on the provision of energy and ICT. Business more generally is also dependent upon ICT services. The ICT sector continues to grow rapidly both in terms of market size and technology itself, leading to an increasing dependence of other sectors on ICT.

Most likely to increase are remote working through wireless devices, cloud-based data storage and the 'invisible' embedding of ICT in the core business processes of every organisation – whether that is 'ticketless travel' on public transport, electronic banking and other financial transactions, or electronic health records. Growth in availability and reliability of ICT will enable the promotion of new working practices, remote working, telecommuting, and working from home.

The shift towards a **low carbon economy** will increase reliance upon the ICT sector. Control of mechanisms such as 'smart grid', offshore generating stations, energy supply and storage (including in electric vehicles) and increasing automation of other elements of the infrastructure (including road traffic management) will be of increasing importance. This will also require more intensive and intelligent use of data for forecasting and managing demand (for energy and other things), especially in relation to weather events.

Transport and travel systems are increasingly reliant upon navigation and control systems operated through ICT, whether that be satellite links, locating beacons, radar, lighthouses, instrument landing and take-off systems for aircraft and airports, satellite-navigation of road vehicles or integrated control systems on rail vehicles. Whilst all might operate in emergency by reversion to local manual control systems, the efficiency of performance would be significantly reduced and safety may be compromised.

Many organisations can cope in the very short-term with a system failure or system outage: they may have back-up manual systems, paper records or alternate delivery plans which enable them to provide a level of service. For business continuity purposes organisations should have regular back up systems and disaster recovery mechanisms in place anyway.

They are often not, though, able to operate 'business as usual' for very long. Under extreme weather conditions, reversion to manual systems may also fail. For example, under normal conditions, many of the switches and routers on the ICT network can be remotely reset enabling management at a distance. During extreme weather events such as heavy rainfall or snow, the damage or failure may be such that remote reset is impossible, e.g. water ingress, at which time reversion to local fixes will be required. This generates two further difficulties:

- *The availability of staff.* Efficiency of business as usual drives down staffing levels to the minimum commensurate with fixing 'normal' problems. Manual reversion requires more staff or longer delays in delivering repairs.
- *The accessibility of the failed element.* This may be limited by the weather event itself (deep snow or flood water) or by the consequences of the failure (e.g. traffic lights have failed and need an engineer on site, but the engineer cannot get to the site because of the traffic jams caused by the traffic light failure).

⁶ AEA (2009) An Overview of Systemic Interdependencies of the UK National Infrastructure, Report to Chief Scientific Advisor of DfT and BIS.

A significant failure of elements of the **ICT in any one geographic region** could also impact on the ability of all other systems to carry out their functions – and because of the non-geographical nature of the distribution of the data elements of the ICT system (data held remotely from users), the impacts are not likely to be geographically constrained. For example, the failure of a data centre in Sheffield, due to over-heating or snow-melt water, would have consequences not just for Sheffield – but for every ICT system user whose data travels through or is held in that centre – regardless of where in the world that user is located.

There may therefore be a ‘local’ issue with users located in that area, but the impacts could ripple out to all inter-connected systems. Whilst the richness of interconnection of ICT will mitigate this to some degree through back up and ‘mirror’ systems, the exact extent of risk and mitigation is actually unknown and probably unknowable. It is unlikely that even the operators of such a centre would be able to define the boundaries to their impacts.

Not only will the need for reliability and availability of ICT increase but also the **demand for the skills** and knowledge to design, build, operate and maintain more sophisticated systems. Jobs lost through automation may increasingly be compensated for by growth in the demand for ICT skills.

These sorts of changes generate an **absolute reliance on the effective functioning of ICT**. Broadband and mobile telephony will become critical to the operation of businesses and access to them will become a fundamental requirement for private housing. Any disruption to ICT services resulting from weather events will become increasingly problematic to individual organisations and users. Enhanced climate resilience to reduce the potential for outages of service may become increasingly important.

Individuals who rely on broadband and telephone connectivity to generate their income may need to invest in greater levels of resilience than they would currently, typically, expect to pay for.

Employing organisations, relying on homeworkers, may need to be willing to invest in providing both the equipment and the connections, offsetting the costs by reduction in the use of office space. The sort of business continuity and disaster recovery plans that are currently put in place within the premises of organisations may need to be extended to cover the infrastructure they rely upon to connect with “agile” workers, wherever they may be.

ICT infrastructure providers will have a key role to play in this issue of business continuity. While providing links to individual homes (and having contracts with individual home occupiers), providers may need to ensure the resilience of their systems can address corporate levels of service and reliability rather than domestic ones.

6 Adaptation in the ICT sector

Adaptation to climate risks will depend upon awareness and action by three groups: by ICT infrastructure and service providers, by all customers reliant on ICT services, and by government to facilitate the market demand for climate resilience. While major ICT providers are able to respond to weather events, there is still a low base of climate change risk awareness, and little evidence that these key organisations are putting in place appropriate climate risk management or adaptation strategies.

A number of generic adaptations apply in the ICT sector, focusing on the enabling role of technology improvements and greater co-ordination and information-sharing between stakeholders in this sector. Specific options to address particular identified climate risks will vary depending upon geographic and business context. A comprehensive approach to dealing with increased climate risks will include actions to reduce vulnerability, improve responses and improve disaster recovery. There are at least five areas for adaptation:

- Enhancing the climate resilience of the network
- Enhancing climate resilience of devices
- Taking advantage of rapidly developing technology
- Improving planning and business processes
- Improving response to weather events

Many potential improvements in climate resilience could offer additional benefits (cost savings, improved efficiency, resource efficiency, etc). Improvement in the ongoing management of the consequences of extreme weather is immediately relevant as it provides current benefits to the ICT sector, as well as the basis for increasing adaptability in the future.

The increasing dependence in coming decades of infrastructure, economy and society on ICT, plus the likely increases in the kinds of weather events which can already disrupt ICT, mean that, from the perspective of those organisations which use and provide services, it will become increasingly important to manage climate risks proactively, efficiently and effectively.

Many improvements in climate resilience frequently offer additional benefits (such as cost savings, improved efficiency, or resource efficiency). In ICT, as elsewhere, adaptation actions to address climate risks will rarely (if ever) be undertaken as a response to climate change alone. Adaptation decisions should not be taken in isolation since they should represent a proportionate response in the context of dealing with the whole range of current and future risks affecting organisations in the sector, whether that is at the level of an individual ICT provider looking to improve the quality of the service it offers, or at the level of an end-user looking to ensure business continuity.

6.1 Adaptation for ICT

Opportunities for building climate resilience in the sector, will involve action on the part of customers, telecommunications and IT service providers, government, and a number of wider stakeholders at national and local levels. We have identified five main areas for action.

6.1.1 Enhancing climate resilience of the network

There are ways in which the resilience of the ICT network could be further enhanced to cope with localised extreme weather hazards. The diversity of systems and their interoperability must be maintained or improved to ensure a level of redundancy sufficient to deal with local events that may rapidly put pressure on, for example, mobile networks, at times of crisis. It may be that further strategic or dynamic nodes could be introduced for specific locations where interconnectivity needs to be allowed under disaster conditions, balanced against cost benefit analysis.

A set of minimum national standards for ICT infrastructure resilience could be considered. These could be used in the planning process to first identify potential areas of weakness and second, to

stimulate adaptation actions. These standards would need to consider not just the resilience of ICT but its implications for other dependent systems in the National Infrastructure.

6.1.2 Enhancing climate resilience of devices

End-user and system devices are not particularly vulnerable to climate changes projected in the UK, because their operating environmental ranges are wider than the conditions we are likely to experience. However, there may be a commercial interest to develop devices and components with higher temperature operating ranges. This form of direct adaptive response for individual devices and components is therefore possible, but unlikely to occur as a response to climate change alone.

The modular approach to infrastructure design in the ICT sector is particularly suited to incremental adaptation, allowing progressively more climate-resilient pieces to be integrated. One other recent advance in technology which is suited to adaptation is the trend towards reprogrammable technologies, which could enable a range of different functions, each tuned to suit the particular environmental conditions encountered during a product's life.

6.1.3 Taking advantage of rapidly developing technology

The pace of technological change in the ICT sector makes it inherently flexible and adaptable, able to respond quickly and cheaply in new generations of devices to the changing requirements of the climate. In order to maximise the potential for adaptation, however, an increased level of climate awareness will be needed within research and development parts of the sector, and more detailed datasets may be required.

It is not only the devices themselves, but whole trends in the sector that can be turned to bring climate adaptation advantages. Virtualisation provides opportunities for enhancing resilience, by, for example, enabling computational load to be transferred from site to site around the globe, avoiding areas of increased weather risk.

6.1.4 Improving planning and business processes

The geographic nature of climate vulnerability in the ICT sector can be addressed through improvements in spatial planning and environmentally-appropriate design. Planning for the location of key buildings, such as data centres, should place a greater emphasis on long term environmental and climate change considerations alongside traditional commercial drivers. There may be a need for mapping and access to relevant data to facilitate this.

It may be possible to tune other business processes to drive a market for increased climate resilience in ICT. Procurement and contractual processes could be used to require an improved level of climate resilience, which emphasises continuity of service rather than compensation for disruption. In turn, this would drive telecommunications and IT service providers to “price in” additional resilience. There might be a need for a government role to unify or coordinate services provided to ensure national interests are represented, as well as reflecting commercial needs.

Organisational protocols for system back-up and information security already exist. Good practice in this regard will also provide resilience, at an organisational level, against disruption from climate events. The adoption of business continuity standards by both providers and consumers of ICT will help, though this may need specific consideration in the context of climate change.

6.1.5 Improving responses to weather events

The telecommunications providers are well equipped to respond to the consequences of environmental disruption to their networks. However, the general approach to weather events seems to be to accept that the risk will occur and then respond to its consequences, rather than a more proactive action seeking to reduce or avoid the risk occurring. With an increasing dependence of all sectors on ICT, and more frequent weather disruptions, this approach may become increasingly expensive, and unsatisfactory from a customer perspective.

Nevertheless, climate resilience may be improved by better response to weather risks. Better contingency planning is needed across a full range of climate hazards, especially those which occur less frequently. Wider use of weather event early warning systems, linking infrastructure providers and operators directly with the Met Office and the Environment Agency (for flood, storm and heat warnings) may help. Better collaboration with local authorities may help to ensure a more efficient and effective recovery phase following weather disruption.

6.2 Challenges and barriers

The challenges and barriers to adaptation are summarised in Table 3. Resilience of ICT infrastructure relies upon the private sector, yet there is a relatively low base of climate change risk awareness among ICT providers and users. We also highlight that it is *only communications* (namely, telecommunications, broadcast and post), and not IT itself, which is considered as national infrastructure and currently included within the Government's Critical Infrastructure Resilience Programme.

Table 3 Summary of some of the challenges and barriers to adaptation in ICT

Challenges and barriers for adaptation in the ICT sector	
Challenges and barriers	Details
Climate change risk awareness and action in the private sector	<ul style="list-style-type: none"> Enhancing the climate resilience of ICT infrastructure relies on the private sector taking action, much more so than in other NI sectors. Telecommunications providers are starting to become "climate risk aware", but much greater awareness across all of the key organisations responsible for ICT infrastructure is needed. Telecommunications and IT companies are generally well-practised at managing risk in their own sector, but may be less effective at considering the implications of risks in related sectors Trends towards a highly-digitised and interconnected world will need systems thinking to manage climate change, and other risks, effectively. Climate risk will also need to be analysed and managed throughout global supply chains.
Current business model for resilience	<ul style="list-style-type: none"> ICT copes with the normal spread of risks to service provision in a robust manner, driven by a business model of 'user pays'. This model has limitations: Customers will only pay for a certain amount of resilience. Similarly, providers trade off the revenue lost from a service outage against the cost of its prevention, and this determines the level of resilience investment made. This model is not well suited to consideration of longer term and uncertain risks, which may be increasing in frequency and/or severity. One step towards improving climate resilience would be the education of system designers about future climate conditions. Solid evidence of the increased likelihood, severity and frequency of extreme weather events is needed. These factors could be built into investment models and additional resilience provided as a function of commercial risk reduction.
Business case for action on climate risk	<ul style="list-style-type: none"> There is a lack of certainty surrounding the magnitude and likelihood of potential climate change impacts and only a very limited evidence base assessing recent experiences of weather events in the ICT sector. There is an underdeveloped "business case" for providers (and customers) to invest in enhanced climate resilience. Infrastructure elements tend to be constructed where greatest demand is located, following changes in the built environment. Integration of adaptation into local planning is needed, considering climate risk to ICT infrastructure alongside the rest of the built environment. Critical elements of the infrastructure should not be developed in locations likely to be increasingly vulnerable to extreme weather events, or if this is unavoidable, planning guidance should ensure that appropriate design standards for the location are applied.
Ownership and sharing	<ul style="list-style-type: none"> The responsibility for securing a resilient communications network at a strategic national level is shared across BIS, Cabinet Office, and Ofcom. However, the responsibility for ensuring reliable and uninterrupted ICT services (particularly IT services) for the users who depend upon them is less clearly defined, in practice being the end result of efforts (not necessarily coordinated) by individual consumers, private sector suppliers and statutory bodies. <i>Only communications</i> (namely, telecommunications, broadcast and post) is considered as NI and included within the Government's Critical Infrastructure Resilience Programme. Thus with regard to planned activity to enhance resilience to natural hazards, IT remains unregulated and unsupported. Commercially, there is an increasing 'sharing' of elements of the infrastructure (e.g., underground cables for data and voice transmission). The 'market' is largely generated by suppliers selling a 'service' based on rebundling bandwidth purchased from the primary

Challenges and barriers for adaptation in the ICT sector	
Challenges and barriers	Details
	infrastructure providers. This sharing needs to become fully transparent to service users such that they understand their risk and exposure, and can take appropriate individual action to spread their risks.
Scale effects	<ul style="list-style-type: none"> • The increasingly virtual nature of ICT services provides a challenge to existing approaches to resilience and dealing with consequences of hazards. • Much of the UK's current approach to strengthening resilience has focused on regional resilience teams and local resilience fora. Some key elements of the UK's ICT (and particularly IT) network may be more difficult to protect under this approach. For example, it may be difficult to prioritise and mobilise local concern to protect a data centre which may have little connection with local communities and yet be of great national importance. • Other technological advances also challenge this approach as data and applications critical to national functions start to be located outside the UK or in areas of international jurisdiction. • Single-sited SMEs are potentially more vulnerable to localised weather-related disruption of their ICT than larger multinational companies. Adaptation also presents a greater challenge to SMEs, both providers and users of ICT.

7 Conclusions and Recommendations

Weather already has the potential to interrupt, or reduce the quality of, ICT services, particularly at the level of an individual end-user.

Climate risks will become an increasing concern for the ICT sector, because of the combination of (a) increasing dependence upon ICT and demand for high quality, uninterrupted, reliable service provision in all areas of business, commerce and leisure, and (b) increasing frequency and severity of the kinds of weather events which can already cause disruption in the sector.

While from the perspective of sustaining critical communications at a national level, resilience to almost all potential climate impacts is likely to remain high, from the perspective of individual end users, the day to day resilience of the ICT services on which they depend is perceived to be lower and more susceptible to localised climate impacts. Climate impacts on ICT can also have considerable cross-sectoral implications for infrastructure and business.

Providers and consumers of ICT will need to consider adaptation. Adaptation options for the ICT sector will enhance the resilience of the infrastructure, take advantage of new technologies and improve business processes. Immediate action can be taken in the areas of research and data development, awareness-raising and engagement, and climate risk management, involving ICT infrastructure providers and ICT consumers, alongside government.

7.1 Conclusions

To some extent, the ICT sector is inherently resilient and adaptable to climate impacts, although this is not necessarily the case at the level of an individual end-user

The vulnerability of the ICT sector to climate change impacts is different in nature and emphasis from the vulnerability of the other national infrastructure sectors (energy, transport, water) considered in the *Infrastructure and Adaptation* project. The vulnerability of the “heavy” infrastructure sectors is strongly linked to their large and often complex physical assets with long lifetimes and long planning timeframes. By contrast, in ICT, the physical assets are not such a liability – apart from buildings and tower structures, the infrastructure is not large, and the components which are the longest-lived – the cables – are very simple and highly resilient.

Thus the climate issues are different: not much of the sector is concerned with long-term planning timeframes in relation to assets. Apart from tower structures, the tunnels through which the fixed cables run and some of the cables themselves, there is very little else that makes up this sector today which we would also expect to see in existence in the 2050s or beyond. Coupled with this, the pace of technology change and development is extremely fast: most sector experts find it hard to look beyond 2030s, let alone out to the end-of-century horizons which climate change forces us to consider.

There are different views about the current level of climate resilience of ICT. From the strategic perspective of the provision of a national emergency communications network, ICT is already to some extent both resilient and adaptable for future climate risks. There are two main reasons for this:

- Multiple alternative networks for communication are available. If one fails, there are usually a number of other options to enable communication.
- The technology is developing rapidly, and much of the infrastructure therefore has short anticipated lifetimes. It is inherently flexible and adaptable, with the possibility for “next generation” devices to be increasingly suited to the climates in which they will be operated. A modular approach to the infrastructure is therefore already in use.

However, from the perspective of an individual end-user or customer, whether a single home-worker, a provider of another national infrastructure service, or a large multinational corporate business, the fact that at national level the telecommunications infrastructure is resilient may be less important than the realities of whether the ICT services on which they rely locally are available and of sufficient quality for their business purposes.

Providers and consumers of ICT will nevertheless need to consider adaptation, because of the UK's increasing dependence on ICT and increases in extreme weather events

Climate trends are important insofar as they provide the backdrop to the sector's technology and behaviour trends over the long-term. The ICT sector continues to grow rapidly both in terms of market size and technology itself. In the coming decades the UK can expect to see the acceleration of current trends for remote working through wireless devices, cloud-based data storage and the 'invisible' embedding of ICT in the core business processes of every organisation. National infrastructure, business and leisure activities are expected to depend increasingly upon uninterrupted ICT services.

Weather already presents disruption and challenge to the provision of services, and increasing dependence on ICT means that the consequences of weather events will become more significant.

Climate risk and resilience in ICT will become an increasing concern primarily because of the increasing reliance of all sectors and business on ICT, but also because the frequency and severity of the kinds of weather events which currently disrupt ICT also look set to increase. The rapid pace of technological change means that the sector has the flexibility to adapt through new technology.

ICT is vulnerable to a number of current and future climate risks, in the UK and internationally

The most significant climate risks to ICT in the UK relate to extreme weather. They include risks related to increasing temperatures, risks related to increases in extreme rainfall and risks related to rising sea levels and increased storm surge. There are some potential benefits relating to projected reductions in snowfall and freezing weather.

The global nature of the ICT sector, including global supply and service chains, means that ICT services in the UK could be affected by climate impacts occurring elsewhere. The sector has links to many parts of the world which are likely to experience more dramatic impacts from climate change than will be seen in the UK (such as India, China, South America, and Siberia). The management of climate risk by providers and users of ICT will need to look closely at these international links.

The consequences of these impacts, alone, or in combination, can be reduced to some key issues:

- Environmental degradation of infrastructure, leading to changes to the expected in-service lifetime of longer-lived structures (such as mobile transmission masts), through changing frequency and intensity of a range of weather events
- Changes to the availability or reliability of ICT services, from disruption caused directly or indirectly by weather events
- Changes to the quality of service provision, particularly connected to the dependence of wireless signal quality on environmental factors (which may be affected by climate change)
- Implications on the needs for repair and recovery following extreme weather damage or disruption in any aspect of the infrastructure, potentially resulting in additional spending required on this aspect of service provision
- Changes to operational business costs (including regular maintenance) in response to environmental factors (for example, heating and air conditioning requirements)
- Changes to working environments (indoor and outdoor) and associated health and safety of employees
- Changes to reliability of international ICT services.

Very few impacts are expected to affect the entire national network, but for individual end-users the localised effects of weather-related disruption are generally expected to increase.

Climate impacts on ICT can have considerable cross-sectoral implications for infrastructure and business

While the ICT sector is dependent upon the provision of energy, all other sectors are dependent upon ICT. Resilience in the ICT sector is critical to the continued operation of the other national infrastructure sectors, and business in general. Direct climate impacts which cause disruption of ICT services can lead to a very wide range of indirect implications in other sectors. To a lesser extent, direct climate impacts elsewhere can have secondary effects on the ICT sector, for example, climate change affecting consumer and business trends, climate change affecting energy security and water availability, weather damage to other structures affecting fixed cables.

The shift towards a low carbon economy will increase reliance upon the ICT sector and will therefore require that it be even more resilient than is currently the case. Control of mechanisms such as ‘smart grid’, offshore generating stations, energy supply and storage (including in electric vehicles) and increasing automation of other elements of the infrastructure (including road traffic management) will be of increasing importance. In this sense, one of the UK’s key policies for climate change mitigation may rely upon appropriate adaptation occurring in the ICT sector.

The implications are that addressing the impacts of climate change on national infrastructure will need a systemic approach. When it comes to the implications of climate impacts on ICT for business, there is a need for individual users, employing organisations and ICT providers to reconsider the needs for increased resilience in future, requiring potentially a greater level of coordination with each other.

Adaptation options for the ICT sector will enhance the resilience of the infrastructure, take advantage of new technologies and improve business processes

Adaptation to the impacts of climate change can range from very generic measures such as increased wealth creation and improved access to technology, to specific options to address particular identified climate risks, to changes which may involve transforming business activities. A comprehensive approach to dealing with increased climate risks will include actions to reduce vulnerability, improve responses and improve disaster recovery.

Improvement in the ongoing management of the consequences of extreme weather is immediately relevant as it provides current benefits to the ICT sector, as well as the basis for increasing adaptability in the future. The study identified five main areas for adaptation in the ICT sector:

- Enhancing the climate resilience of the network
- Enhancing climate resilience of devices
- Taking advantage of rapidly developing technology
- Improving planning and business processes
- Improving response to weather events

We may see some transformative adaptation within the sector, largely because of the pace of technology development, if climate concerns can be drawn into future thinking, research and development. There are some unique opportunities for building climate resilience in ICT. Virtualisation (e.g., cloud computing) provides a unique way in which the sector can transfer risk away from local climate impacts, but this will depend on good early-warnings and even higher maintenance of connectivity with the end users.

The modular approach to infrastructure design in the ICT sector, necessitated mainly to suit the wide range of lifetimes of components, as well as the rapid pace of technological change, is particularly suited to incremental adaptation, allowing progressively more climate-resilient components to be integrated into the infrastructure.

There will be an important role for ICT infrastructure providers and ICT consumers, alongside government, in overcoming the barriers to adaptation

Enhancing the climate resilience of national infrastructure for ICT relies on the private sector taking action, much more so than in other national infrastructure sectors. There is a relatively low level of “climate risk awareness” among ICT infrastructure providers compared to the other national infrastructure sectors.

The current model for resilience in the sector emphasises the provision of levels of resilience sufficient for “business as usual”, paid for by customers. With climate change and trends within the sector, this model may not deliver any necessary increase in resilience, since it would rely upon both system designers and customers to factor in the potential impacts of climate change. The business case for action on climate risk, both for ICT providers and users, is poorly developed: there is only a limited evidence base assessing recent experiences of weather events in the sector, and no research modelling the scale and cost of future events.

The responsibility for ensuring that reliable and uninterrupted ICT services (particularly IT services) are extended to the wide range of users who depend upon them is poorly defined, in practice being

the end result of efforts (not necessarily coordinated) by individual consumers, private sector suppliers and statutory bodies. This is a greater challenge looking beyond the ICT sector: while telecommunications companies are well-practised at managing their own risks, they are less effective at considering the implications of risks in related sectors. Underlying trends towards a highly-digitised and interconnected world will need systems thinking to manage climate, and other risks effectively.

7.2 Recommendations

The study offers recommendations in the following areas:

- Research and data development
- Awareness-raising and engagement within the ICT sector
- Engagement outside the ICT sector
- Climate risk management

These are summarised in Table 4, which also suggests which actors should be involved in each.

Table 4 Study recommendations with suggestions of who should be involved

Summary of study recommendations identifying the relevant actors				
Recommendation	Government	ICT providers	ICT customers	Research community
Research and data development				
Detailed follow-up assessment of direct climate change risks	✓			✓
Evidence review of the impact of past weather events on infrastructure and ICT service providers	✓	✓		
Specific research questions on climate change projections (absolute humidity; potential changes in wireless signal)				✓
Policy study to review the potential role of government, the regulator, and existing market structures in addressing climate risks in the ICT sector	✓	✓	✓	
Awareness-raising and engagement within the ICT sector				
Activities to raise awareness within the ICT sector of the potential impacts of climate change, through the <i>Infrastructure and Adaptation</i> project	✓	✓	✓	
Workshops or collaborative efforts among the major telecommunications providers to build the business case for companies themselves to address climate risks		✓		
Engagement within the sector to review models for ownership, roles and responsibilities in the context of climate resilience	✓	✓	✓	
Horizon-scanning exercise to scope the long-term trends in the ICT sector and compare with climate change	✓	✓	✓	✓
Engagement outside the ICT sector				
Cross-Government collaboration to explore interdependency issues	✓	✓	✓	
Better coordination of emergency response and local authority resilience plans with ICT providers	✓	✓		
Further investigation of supply chain security for ICT, including international dimension		✓		✓
Climate risk management in the ICT sector				
Consider how the IT industry may be drawn into the Critical Infrastructure Resilience Programme in future, alongside telecommunications infrastructure	✓			
Corporate climate risk management programmes (in the context of their wider risk management strategies)		✓	✓	
Greater use of weather-forecasting data for early-warning, and link into Environment Agency flood warnings		✓		
Ongoing work to improve contingency and emergency recovery plans should be extended to cover a full range of weather events, and to consider how climate change	✓	✓	✓	
Customers of ICT services to become more aware and demanding of climate resilience	✓		✓	



AEA group
329 Harwell
Didcot
Oxfordshire
OX11 0QJ

Tel: 0870 190 3862
Fax: 0870 190 6318