AEA

Adapting the ICT Sector to the Impacts of Climate Change

Final Report

ED49926
Issue 5
August 2010

Title	Adapting the ICT Sector to the Impacts of Climate Change – Final Report
Customer	Defra
Customer reference	RMP 5604
Confidentiality, copyright and reproduction	Crown Copyright 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.
File reference	ED49926
Reference number	ED49926 - Issue 5

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, Clare Downing, Richard Davey, Aisling O'Sullivan
Approved by	Name	Geoff Dollard
	Signature	
	Date	29 August 2010

Disclaimer

Adapting the ICT Sector to the Impacts of Climate Change – Final 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 an earlier version of this report.

Citation

This report should be cited as:

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

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.

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).

Nevertheless, climate risks will become an increasing concern, 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.

Adaptation will, therefore, be needed. Additionally, 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.

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. Many of these are linked to the projected increase in winter temperatures and reducing likelihood of snowfall, with its implications for damage to infrastructure and disruption to maintenance and repair schedules. 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, perhaps, is the potential knock-on of even some localised disruption to ICT services on interdependent infrastructure and business sectors.

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.

There are some barriers to adaptation in the ICT sector. The study has identified several challenges, and these include:

- A low base of climate change risk awareness among ICT providers and users, with a consequent lack of adaptation action;
- A current business model for resilience which is not well suited to consideration of longer term and uncertain risks;
- A very limited evidence base assessing recent experiences of weather events in the sector and therefore an underdeveloped “business case” for providers (and customers) to invest in adaptation;
- An increasing trend towards sharing of elements of the infrastructure by several service providers; and
- The increasingly virtual nature of ICT services, which may be physically located outside the UK.

Additionally, we highlight that it is *only communications* (namely, telecommunications, broadcast and post) which is considered as national infrastructure and currently included within the Government's Critical Infrastructure Resilience Programme, and not IT. Consequently IT remains unregulated and unsupported in enhancing its resilience to natural hazards, including climate change

There may be potential for equity issues related to the impacts of climate change in the ICT sector, with adaptation presenting a greater challenge to SMEs than to large multinational organisations, both the providers and users of ICT.

We offer recommendations relating to research, engagement and awareness raising, and climate risk management, as shown in the table.

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 *Infrastructure and Adaptation* 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	✓		✓	

Table of contents

Appendices

1 Introduction

The impacts of climate change will affect our national infrastructure. This is recognised in the cross-Government Adapting to Climate Change (ACC) Programme which has prioritised adapting national infrastructure.

In addition, the Council for Science and Technology report 'A National Infrastructure for the 21st century' (CST, 2009) recognised that resilience against climate change is the most significant and complex longer-term challenge facing our national infrastructure. Similarly, the Government's update to the National Security Strategy, (Cabinet Office, 2009), recognised climate change to be a priority driver of threats to national security, given expected world-wide and domestic impacts.

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. The UK's national infrastructure, including ICT (Information and Communication Technology), is vulnerable to many of these changes, and rather than long-term average increases it is change in the nature and frequency of extreme events that are of particular concern. Given the dependence both upon and by multinational organizations, international markets and global supply chains, the UK telecommunications/ICT sector is potentially at risk from the impacts of climate change occurring elsewhere in the world.

1.1 Climate change policy context

The Climate Change Act (2008) made the UK the first country in the world to have a legally binding long-term framework to cut carbon emissions. It also created a framework for building the UK's ability to adapt to climate change. It includes a number of duties related to adaptation. Of relevance to this study are:

- a UK-wide climate change risk assessment (CCRA) must take place every five years (with the first CCRA to be laid before Parliament by January 2012);
- a national adaptation programme must be put in place and reviewed every five years to address the most pressing climate change risks to England (with the first to be laid before Parliament as soon as reasonably practical after the completion of the CCRA);
- 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 Government published its strategy outlining how the Reporting Power would be used in November 2009, and this identified a focus on organisations responsible for national infrastructure. The potential vulnerability of the ICT sector to climate change risks is underlined by the fact that Ofcom is listed as a priority reporting authority in the strategy, and that other organisations within the ICT sector will be encouraged to report voluntarily.

The ACC Programme is co-ordinated by Defra and aims to:

- develop a more robust and comprehensive evidence base about the impacts and consequences of climate change.
- raise awareness of the need to take action now and help others to take action.
- work across Government at the national, regional and local level to make sure the need to adapt to climate change is embedded into Government policies, programme and systems
- evaluate progress and take steps to ensure effective delivery of the Programme's objectives.

1.2 Project context

This work has been undertaken as part of the ACC's cross-departmental *Infrastructure and Adaptation* Project; a two-year project (ending March 2011) to identify and examine strategic solutions to increase the long-term resilience of energy, ICT, transport and water infrastructure to future climate change impacts.

An initial study under the *Infrastructure and Adaptation* Project explored how to increase the long-term resilience to climate change of infrastructure in the energy, transport and water sectors (URS, 2010). The study which is the subject of this report has focused on climate change and its impacts on the ICT sector. There is as yet very little prior work which specifically considers the potential impacts of climate change on ICT, the sector's vulnerabilities or possible adaptation, 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".

1.2.1 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

1.2.2 Scope of the study

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 inasmuch as it impinges upon the ICT services used in the UK. Appendix 1 provides an outline of the study methodology, which included an ICT sector expert workshop. The report of the workshop is provided in Appendix 2.

For the purposes of this report, ICT is taken to mean the whole of the networks, systems and artefacts which enable the transmission, receipt, capture, storage and manipulation of voice and data traffic on and across electronic devices.

The concept of resilience is used in many contexts.

> In the Critical Infrastructure Resilience Programme, resilience is defined as "the ability of a system or organisation to withstand and recover from adversity". A resilient organisation is one that is still able to achieve its core objectives in the face of adversity through a combination of measures (Cabinet Office, 2010).
>
> In the context of climate impacts, the UK Climate Impacts Programme[1] 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".
>
> A definition used to emphasise the interdependencies of national infrastructure is: "An infrastructure element is resilient when, although dependent on other systems, it can continue to function effectively when one or more of those dependencies are broken. It can do this because there are multiple paths to enable its operation such that no single dependency failure can prevent its operation."

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

For the purposes of this report, we restrict ourselves to the 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.

Further definitions are provided in the Glossary at the end of this report.

2 The ICT sector in the UK

In this chapter, we offer an overview of the ICT sector, its role in the UK economy and possible future trends.

2.1 Introduction to ICT

Within this project, ICT is 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 of this study, 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, because of that and the need to address commercial imperatives, both user and system devices are designed to conform to industry agreed standards (IEEE) 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. ICT is the only sector of infrastructure that directly connects any one user to any other user across time and space using multiple pathways simultaneously and capable of dynamic re-routing in real time. As such, in this case, the national asset is the network rather than any of the individual components – and it is the operation of the network that relies on the whole infrastructure and enables the generation of value.

2. 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 – streams of moving 'bits' – separated into 'data packets' at one end of their journey and reassembled at the other. Thus the whole of data and voice is converging as are the devices from which the messages are sent and received. At the level of this report there is no meaningful difference between them. A further emergent complexity in this case is the growth of 'power over ethernet' in which the network cable that carries data is also used to carry electricity. From this emerges a further convergence of the ICT sector with, elements of, the energy system increasing their interdependence and co-functionality in which either they both work or neither works.

3. 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 streams of digital data in close to real-time – whether it is the extraction of cash from an ATM, the use of a credit or debit card,

sending an email, controlling a remote pump or switch, despatching or receiving aircraft or a mundane phone call.

All of the value that may be generated through any one of those activities is utterly reliant 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 in the UK

ICT is central to the 'business as usual' operation of every industry and sector and, whilst a generation ago, much of the hardware and software classed as the "ICT sector" was technically challenging and for use by specialists only, the contemporary world is almost blind to its existence. Like water from a tap, the core assumption is that the ICT is 'always available'. We pick up the phone, send email, enter data in applications and databases, unconscious to the technology which enables it – and unaware of its complexity, resilience or fragility. Intellect (2010) estimates that 4.2 million people in the UK work flexibly: the vast majority of these use broadband and other technology to work remotely, balancing home and work life. The sector employs over 5 million people in the wider knowledge industries and over one in twenty of the UK workforce is an IT professional. Thus, while the sector includes primarily those organisations which provide ICT infrastructure and services, there is a sense in which all organisations and individuals which rely on ICT for day to day functions are key stakeholders in the sector. Table 2.1 provides some statistics to demonstrate the role that ICT plays in our lives today.

Table 2.1 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
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
Estimates suggest the ICT sector was responsible for around 2% of global carbon dioxide emissions in 2007
The Energy Savings Trust in 2007 predicted that 45% of domestic energy usage would be consumed by ICT
98% of UK businesses rely on technology to power their day-to-day operations.
Estimates say 84% of UK businesses are heavily dependent on their IT systems. (PwC Information and Security Survey, 2008)
Intellect estimate 4.2 million people in the UK work flexibly - the vast majority of these use broadband and other technology to work remotely
The *Digital Britain* sectors account for nearly £1 in every £10 that the whole economy produces each year
Six of the top 10 global brands by value this year are in the digital sector
The IT professional workforce, alone, in the UK has almost doubled in the last 12 years: from 550,000 to around one million today
Over the next five years, the UK will require more than 140,000 new IT and Telecoms professionals per year
On 15 June 2009, 20 hours of new content were posted on YouTube every minute, 494 exabytes of information were transferred seamlessly across the globe, over 2.6 billion mobile minutes were exchanged across Europe, and millions of enquiries were made using a Google algorithm.
In the high street, stock ordering, inventory control and the cash tills are all completely dependent on electronic communications
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
Sources: Department for Culture, Media and Sport and Department of Business Innovation and Skills (2009) *Digital Britain* Intellect (2010) *General Industry Fast Facts* http://www.intellectuk.org/content/view/4348/377/#general

During normal times, as the following extract from the IEEE standard for Local and Metropolitan Networks shows, telecommunications / ICT is typically highly reliable (IEEE Computer Society, 2002). This extract describes the acceptable error rate (loss of data) for transmissions in a properly designed, configured, installed and maintained network:

> *the risk of error for wired or optical fibre physical media shall be less than 8 × 10^{-8} per octet, and for wireless physical media it shall be less than 8 × 10^{-8} per octet. The probability that an MSDU delivered at an MSAP contains an undetected error, due to operation of the MAC service provider, shall be less than 5 × 10^{-14} per octet of MSDU length or approximately 1 in 13 300 000 000.*

Whilst describing transmission of one particular element of the network, the standards are of necessity, consistent. The probability of a lost data packet is very very small.

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 generate potential single points of failure. For example, if data traffic from a particular country or location is completely lost for any reason, the local services which rely on it will cease to be available (the ICT equivalent of turning off the trans-european gas pipeline).

New generations of infrastructure artefacts (e.g. rail vehicles, signalling systems, the ‘smart-grid’, water treatment plants) are embedding ever greater numbers of localized computing devices communicating with each other and with their remote controllers via the internet, which is also carrying increasing amounts of voice traffic through ‘VOIP’ telephony systems. The wider elements of the UK’s National Infrastructure are increasingly reliant for operation on a complex web of above and sub-ground connectivity. Above ground systems are vulnerable to wind and precipitation whilst below ground systems are vulnerable particularly to ground water and subsidence. Resilience of these sectors would be significantly enhanced if they more fully recognised the potential risks and engaged directly with the appropriate parts of the ICT industry with regard to resilience.

For example, the power generation and distribution system, particularly as it comes to utilize power from renewable sources, will need significant data flows to know who and what is drawing and providing power where, and how that power needs to be managed, paid for and charged for: a massive increase in reliance on both the infrastructural and informational layers of ICT. Similarly, ‘live trains’ (a project underway in the Department for Transport) will be capturing real-time information about train performance (across up to 60 channels per train) in order to provide information to passengers, engineers and managers. These things will continue to increase the workload placed on ICT infrastructure, which in turn relies on the availability of energy for operation.

A recent study of the interdependencies in UK national infrastructure found that of all the sectors examined, ICT has the least reliance on other sectors for the operation of its services; the industry with the highest number of interdependencies (reliance on other industries) is energy, having 17 interactions whilst transport and waste have 16 (AEA, 2009a). ICT has the least reliance with 7, while water has 6. However, ICT is of course wholly reliant on the energy sector. Both ICT and energy were identified as Critical Infrastructure sectors by the European Programme for Critical Infrastructure Protection.

In the recent report to the *Infrastructure and Adaptation* project, some key interconnections between ICT and energy, transport and water sectors were documented (URS, 2010):

- Key ICT Services to the Energy Sector: ICT provides a critical operational service for much of the UK energy infrastructure; both at individual plants and also across networks where it supports supply and demand forecasting and re-routing of gas and electricity supplies through the transmission and distribution networks. Further developments in the energy sector in the next decades, including increased uptake of Government support for localised micro generation renewable energy schemes, are anticipated to further increase the reliance on ICT.

- Key ICT Services to the Transport Sector: ICT provides a critical operational service for much of the UK transport infrastructure, from road information on the motorway network through to air traffic control. This reliance on ICT is also likely to increase into the next decades. Those maintaining the road network also tend to rely heavily on mobile phones. At times of major disruption, such as the snow event in January 2003 on the M11, the loss of a signal, due for example to communication masts being put out of action, can cause much greater operational difficulties.

- Key ICT Services to the Water Sector: ICT in the water sector primarily consists of personal communication with staff (land lines, mobile phones, two-way radio, etc), internet and intranet services as well as telemetry including some control of remote assets. Many pumping stations and treatment works will have internal SCADA systems. Climate change impacts on any of these modes of communication and data transfer will affect the operation of water and wastewater infrastructure and have the potential for disruption or failure of water supply or wastewater treatment provisions.

2.3 Ownership, legislation and regulation

2.3.1 Structure and ownership of the ICT sector

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.

CST (2009) states that the dominance of a small number of IT component subsystem suppliers, such as Microsoft, Google, Cisco and Intel, has resulted in vulnerabilities within ICT which may increase risks of cascade failure and/or reduce resilience. As the whole system becomes increasingly dependent upon a small number of major suppliers, the disruption resulting from production of an inadequate or vulnerable component which is widely or universally used can be extremely widespread; issues have, for example, been seen with operating systems, batteries and charging devices.

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.

Given how much it underpins the rest of the NI, it is crucial to ensure that ICT is developed in a manner that not only meets the needs of the market and the consumer, but also addresses the broader strategic objectives of Government in terms of coherence and resilience. Widespread disruption or failure of these systems would have catastrophic effects. Simply assuming 'the market will provide' may not be enough.

2.3.2 Legislative and regulatory context

Legislation and regulation is primarily focused on the use of services in the ICT sector, relating to topics such as piracy, customer pricing and access to facilities. Regulation outside of the areas of energy use and efficiency, particularly in terms of environmental regulations and resilience to environmental impacts, is scarce. The system of detailed market definition and reviews, assessment of significant market power and detailed remedies, created by the series of European Communications Directives, was transposed into UK legislation but deals with little in this area.

In the UK, there are several aspects of Government's work designed to enhance the resilience of national infrastructure to environmental impacts.

- Ofcom
- The Digital Economy Act
- The Pitt Review
- The Cabinet Office Critical Infrastructure Resilience Programme

Ofcom

Ofcom is the independent regulator and competition authority for the UK communications industries, with responsibilities across television, radio, telecommunications and wireless communications services. Ofcom operates under the Communications Act (2003) with general duties to further the interests of citizens and of consumers.

Ofcom's main specific duties include ensuring the UK has a wide range of electronic communications services, a range of high quality programmes available, and that there is competition in the market.

Ofcom has very few duties related to resilience and its regulation. The Digital Economy Act (2010) requires Ofcom to provide a report on the state of the UK's telecoms infrastructure every three years, and this includes an account of preparations made by network and service providers to respond to emergencies. Ofcom regulates General Conditions of Entitlement[2] (which apply to anyone who provides an electronic communication service or an electronic communications network), and General Condition 3 requires providers of public telephone networks or publicly available telephone services (excluding mobile networks or services) to "take all reasonable steps to ensure the proper and effective functioning of the public telephone network at all times, including the availability of the network and service in the event of catastrophic failures, and to ensure uninterrupted access to emergency services".

Ofcom currently undertakes virtually no discernable tasks in relation to climate resilience of national infrastructure. However, Ofcom will be required to produce a report to Defra's Secretary of State on climate risks and adaptation under the Adaptation Reporting Power by September 2011.

Digital Economy Act, 2010

The Digital Economy Act became law on 8 April 2010. The Act implements aspects of Government policy on digital media set out in the 'Digital Britain' White Paper[3] (2009). Amongst other things, it enforces a new duty on Ofcom to report to the Secretary of State on the UK communications infrastructure every three years. The initial report and the three-yearly reports will consist of a survey of:

- The different types of electronic communications network and service in the UK;
- Geographic and population coverage of those networks and services;
- Downtime, and measures in place to maintain or improve availability;
- Emergency planning; and
- A comparison between UK networks and services and equivalent networks and services provided in a range of other countries.

The Pitt Review

The Pitt Review into the 2007 floods considered how the resilience of critical infrastructure to similar flood events might be improved. Amongst the Review's final recommendations were five which seek to improve the resilience of critical infrastructure and essential services to disruption from natural hazards, and which are of relevance to the ICT sector and climate resilience:

[2] When the EU communications regime was implemented in the UK in 2003, individual licences granted under the Telecommunications Act 1984 were replaced by the General Authorisation regime. The effect was that licences are no longer required for providing communications networks or services in the UK – everyone is 'generally authorised' to do so. However, the General Authorisation is subject to the General Conditions of Entitlement: these conditions apply to all persons providing electronic communications networks and services.

[3] *Digital Britain* outlines the Government's strategic vision for ensuring that the UK is at the leading edge of the global digital economy.

- Recommendation 50: The Government should urgently begin its systematic programme to reduce the disruption of essential services resulting from natural hazards by publishing a national framework and policy statement setting out the process, timescales and expectations.

- Recommendation 51: Relevant government departments and the Environment Agency should work with infrastructure operators to identify the vulnerability and risk of assets to flooding and a summary of the analysis should be published in Sector Resilience Plans.

- Recommendation 52: In the short-term, the Government and infrastructure operators should work together to build a level of resilience into critical infrastructure assets that ensures continuity during a worst case flood event.

- Recommendation 53: A specific duty should be placed on economic regulators to build resilience in the critical infrastructure.

- Recommendation 54: The Government should extend the duty to undertake business continuity planning to infrastructure operating Category 2 responders to a standard equivalent to BS 25999, and that accountability is ensured through an annual benchmarking exercise within each sector.

These recommendations are being delivered by the Natural Hazards team in the Cabinet Office.

The Cabinet Office Critical Infrastructure Resilience Programme (Natural Hazards Team)

The Natural Hazards Team was created in May 2009 to establish a cross-sector programme to deliver recommendations 50 – 54 from Sir Michael Pitt's report on the 2007 floods.

A Strategic Framework and Policy Statement for the cross-sector Critical Infrastructure Resilience Programme (CIRP) was finalised and published in March 2010 (Cabinet Office, 2010a). It sets out the process, timetable and expectations for the resilience programme. The purpose is to develop a shared, consistent, proportionate and risk-based approach to delivering reductions in vulnerability over a number of years. The Framework is primarily directed at central government departments, regulators, relevant public sector bodies and critical infrastructure owners. It aims to:

- Embed a co-ordinated and systematic approach to improve resilience of the infrastructure network and systems that provide essential services to severe disruption from natural hazards.
- Establish an interim minimum standard for resilience to flooding.
- Clarify the roles and responsibilities of the wide range of public and private sector bodies who will contribute to the delivery of the shared goals of the Programme

The aims of the Critical Infrastructure Resilience Programme are to:

- Reduce the most substantial risks to the continuity of critical infrastructure and essential services resulting from severe disruption caused by natural hazards, through the careful assessment of vulnerability and prudent and proportionate risk mitigation activity based on new, centrally-defined standards.
- Provide a shared framework to support cross-sector activity to assess, enhance and sustain the resilience of critical infrastructure and essential services to disruption from natural hazards.
- Enhance the collective capacity of critical infrastructure to absorb shock and act quickly when faced with unexpected events.
- Ensure an effective emergency response at the local level through improved information sharing and engagement before, during and after emergencies.

The Cabinet Office emphasizes that resilience encompasses activity to prevent, protect and prepare for natural hazards. The programme to improve resilience of the UK's critical infrastructure will encompass prevention, protection, response and recovery. It will also need to take account of dependencies and interdependencies within and between sectors.

The Natural Hazards Team has also published the Sector Resilience Plan for Critical Infrastructure summarising the vulnerability of critical national infrastructure in each sector, and plans to improve resilience (Cabinet Office, 2010b). Alongside the plan, initial guidance to the water, energy, transport and telecommunications sectors has been produced (Cabinet Office, 2010c).

The Critical Infrastructure Resilience Programme covers communications networks, broadcast and post. The critical infrastructure supplying UK communications networks is not subdivided further into telecoms and IT, but regarded as one complex network which may support a number of different functions.

2.4 Resilience in the ICT sector

It is in the interest of ICT providers, in an extremely competitive market, to maintain service by ensuring a good level of resilience. The ability to switch between the major networks, combined with industry and Government cooperation to mitigate against disruption to telecoms services, has ensured a good level of inherent resilience. This has mainly come about as a consequence of the actions of individual companies. BIS continues to work with the sector as a whole to enhance overall resilience, in relation to flooding, and sharing good practice on denial of access. This is expected to continue, with company reporting on overall resilience forming part of the requirements of Article 13 of the European Framework Directive of the Electronic Communications Framework Review[4]. In addition, the network is continually improving. The transition to 21st century networks is replacing copper cables with fibre optic cables, which can carry more information making it easier to re-route large volumes of calls over the network if there is a failure in one part of it. Resilience activity has been driven by an ongoing commitment to maintain and improve resilience, as well as an ability to react quickly to individual incidents resulting in, for example, the reassessment of cabling locations and alternative back-up capacity

The Cabinet Office considers that resilience of national infrastructure in the telecommunications sector is conferred by (Cabinet Office, 2010b):

- 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.

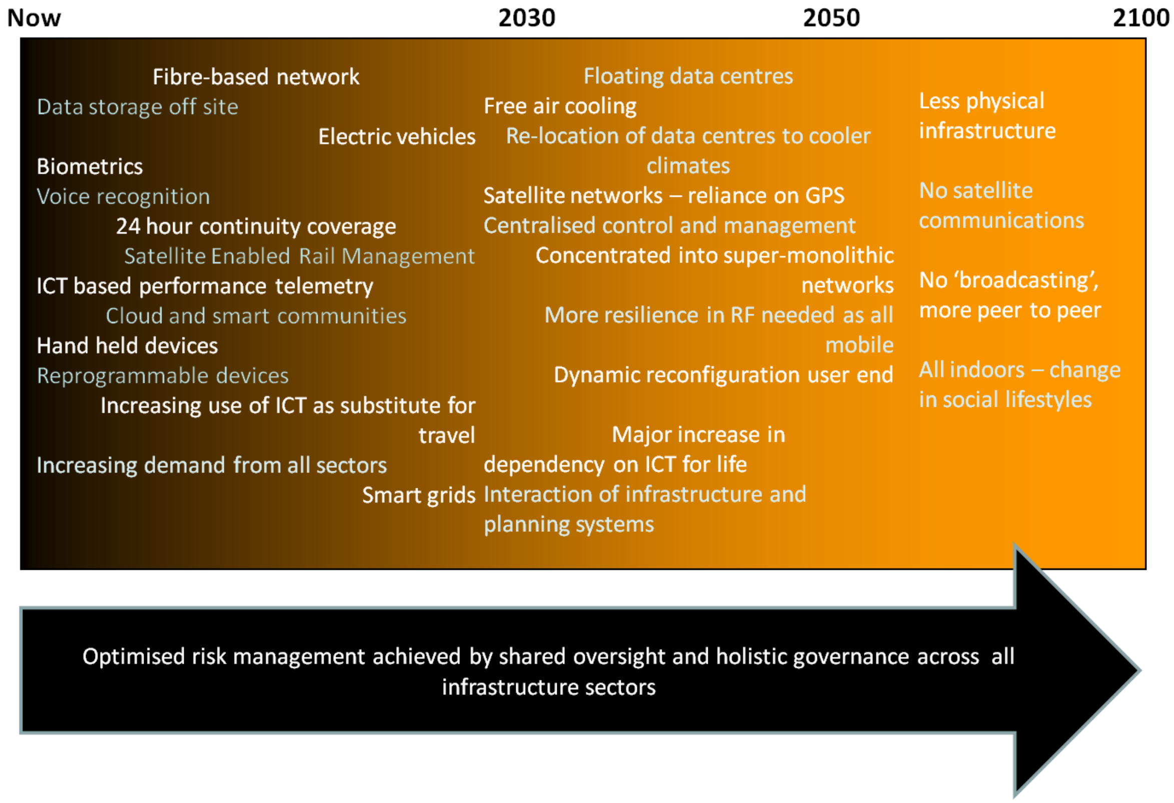
For the purposes of this study, we highlight that while *from the perspective of maintaining critical communications* at a national level, the sector is to an extent inherently resilient to current and future climate impacts, *from the perspective of the consumer*, what actually matters is the loss of 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. Appendix 3 provides one model for resilience to illustrate this.

2.5 Future trends in the ICT sector

The ICT sector continues to grow rapidly both in terms of market size and technology itself. Figure 2.1 illustrates potential trends within the sector, as identified during the expert workshop.

[4] DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009, amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, text published in the Official Journal of the European Union, Volume 52 (18 December 2009).

Figure 2.1 Illustration of potential trends and technology developments in the ICT sector through this century


Now
2030
2050
2100
Fibre-based network
Data storage off site
Electric vehicles
Biometrics
Voice recognition
24 hour continuity coverage
Satellite Enabled Rail Management
ICT based performance telemetry
Cloud and smart communities
Hand held devices
Reprogrammable devices
Increasing use of ICT as substitute for travel
Increasing demand from all sectors
Smart grids
Floating data centres
Free air cooling
Re-location of data centres to cooler climates
Satellite networks – reliance on GPS
Centralised control and management
Concentrated into super-monolithic networks
More resilience in RF needed as all mobile
Dynamic reconfiguration user end
Major increase in dependency on ICT for life
Interaction of infrastructure and planning systems
Less physical infrastructure
No satellite communications
No 'broadcasting', more peer to peer
All indoors – change in social lifestyles
Optimised risk management achieved by shared oversight and holistic governance across all infrastructure sectors

In as much as customers keep purchasing (and increasing their spending) on all forms of communication, the sector can be expected to maintain a high level of resilience as a purely commercial activity. Customers demand very high levels of service availability and quality and thus the sector is incentivised to maintain those characteristics. From the provider perspective, there is an ongoing wish to increase cost-efficiency of service provision so again, the industry can be expected to maintain a level of investment in resilience that drives performance.

Demand is likely to increase for provision of fibre-optic networks since these are faster and more reliable than the copper based networks – some of which are reportedly more than 70 years old. Both of these may be subject to climate change impacts.

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. Looking at this in terms of the opportunity, growth in availability and reliability of ICT will enable the promotion of new working practices, remote working, telecommuting, working from home, which offer the potential for reduction in carbon emissions through reduced travel and reduced demand for office space. All of this is possible within the bounds of known ICT solutions, but the maintenance of systemic resilience is crucial to its success.

Looking towards the 2050s, it is expected that current trends will continue towards ever larger, perhaps ever more remote data centres, probably owned by a smaller number of very large service providers (reflecting trends in the motor manufacturing and banking industries). In this projection the management and protection of the UK resilience in ICT will become a matter of global concern. The systems are believed to be able to cope, but there is a political/social dimension which will need to be addressed.

Going beyond that period it is meaningless to project anything of substance. The rate of the development of intellectual property in this sector shows no sign of abating. The emergence of cloud computing is anticipated to be followed by 'nano-technology', the capabilities and power consumption characteristics of which are as yet unknowable – although the predictions are for massively increased speed and substantially reduced power consumption. However, the increase in use overall might be expected to absorb the reduction in consumption of individual devices.

3 Headline climate change messages for ICT

This chapter provides an overview of climate change as relevant to a consideration of climate risks in the ICT sector. This information is the basis for the discussion in subsequent chapters.

3.1 Recent trends in UK climate

Average temperature across all regions of the UK has risen since the mid 20th century, as have average sea level and sea surface temperature around the UK coast. Over the same time period, trends in precipitation and storminess are harder to identify.

Table 3.1 summarises key results from studies of recent trends in UK climate by the UK Climate Impacts Programme and the Met Office (Jenkins et al., 2009).

Table 3.1 Recent changes in UK climate

Recent trends in UK climate	
Climate variable	Observed trend
Temperature	• Central England Temperature has risen by about 1 °C since the 1970s, with 2006 being the warmest year on record. It is likely that there has been a significant influence from human activity on this recent warming. • Temperatures in Scotland and Northern Ireland have risen by about 0.8 °C since about 1980.
Precipitation	• Annual mean precipitation over England and Wales has not changed significantly since records began in 1766. • Seasonal rainfall is highly variable, but appears to have decreased in summer and increased in winter, although with little change in the latter over the last 50 years. • Over the last 45 years, all regions of the UK have experienced an increase in the contribution to winter rainfall from heavy precipitation events; in summer all regions except North East England and Northern Scotland show decreases. • South East England has seen the greatest decline in the number of days of rain annually, leading to increased drought conditions
Storms	• Severe windstorms around the UK have become more frequent in the past few decades, though not above that seen in the 1920s.
Sea level rise	• Sea level around the UK rose by about 1mm/yr in the 20th century, corrected for land movement. The rate for the 1990s and 2000s has been higher than this.
Sea surface temperature	• Sea-surface temperatures around the UK coast have risen over the past three decades by about 0.7 °C.

There are extremely clear trends in UK annual average temperatures, indicating the scale and rate of climate change that we are now facing. Recent observations of rainfall show smaller changes, with only a slight trend for increased rainfall in winter and decreased rainfall in summer detected over the last 250 years. However, one clear trend is that all regions of the UK have experienced an increase in the amount of winter rain that falls in heavy downpours.

3.2 Future projections of climate change in the UK

The UK Climate Projections provide probabilistic information about climate change in the UK over the 21st century (Murphy, et al., 2009). The projections over land are provided for three emissions scenarios based on the Intergovernmental Panel on Climate Change’s (IPCC) Special Report on Emissions Scenarios (SRES): low (B1), medium (A1B) and high (A1F1), at 25 km resolution and for administrative regions and river basins. These land projections are also reported for seven overlapping 30-year time periods from the 2020s (2010-2039), to the 2080s (2070-2099), where each future time period is named after the decade upon which it is centered.

In Table 3.2 we summarise expected changes under the medium emissions scenario by the 2080s (relative to the 1961–1990 baseline). The figures provided are the central estimates of change (those at the 50% probability level) followed, in brackets, by changes which are very likely to be exceeded, and very likely not to be exceeded (10% and 90% probability levels, respectively). For sea level rise, only the central estimate is quoted.

Table 3.2 Headline messages from the UK Climate Projections (medium emissions scenario)

Climate projections for the 2080s under the medium emissions scenario (UKCP09)	
Climate variable	Projection
Temperature	• Average temperature increases in all areas of the UK, more so in summer than in winter. Changes in summer mean temperatures are greatest in parts of southern England (up to 4.2ºC (2.2 to 6.8ºC)) and least in the Scottish islands (just over 2.5ºC (1.2 to 4.1ºC)). • Mean daily maximum temperatures increase everywhere. Increases in the summer average are up to 5.4ºC (2.2 to 9.5ºC) in parts of southern England and 2.8ºC (1 to 5ºC) in parts of northern Britain. Increases in winter are 1.5ºC (0.7 to 2.7ºC) to 2.5ºC (1.3 to 4.4ºC) across the country. • Changes in the warmest day of summer range from +2.4ºC (–2.4 to +6.8ºC) to +4.8ºC (+0.2 to +12.3ºC), depending on location, but with no simple geographical pattern • Mean daily minimum temperature increases on average in winter by about 2.1ºC (0.6 to 3.7ºC) to 3.5ºC (1.5 to 5.9ºC) depending on location. In summer it increases by 2.7ºC (1.3 to 4.5ºC) to 4.1ºC (2.0 to 7.1ºC), with the biggest increases in southern Britain and the smallest in northern Scotland.
Precipitation	• Central estimates of annual precipitation amounts show very little change everywhere at the 50% probability level. Changes range from –16% in some places at the 10% probability level, to +14% in some places at the 90% probability level, with no simple pattern. • The biggest changes in precipitation in winter, increases up to +33% (+9 to +70%), are seen along the western side of the UK. Decreases of a few percent (–11 to +7%) are seen over parts of the Scottish highlands. • The biggest changes in precipitation in summer, down to about –40% (–65 to –6%), are seen in parts of the far south of England. Changes close to zero (–8 to +10%) are seen over parts of northern Scotland. • Changes in the wettest day of the winter range from zero (–12 to +13%) in parts of Scotland to +25% (+7 to +56%) in parts of England • Changes in the wettest day of the summer range from –12% (–38 to +9%) in parts of southern England to +12% (–1 to +51%) in parts of Scotland.
Storms and wind	• The UK Climate Projections do not include projections of wind speed. The Met Office Hadley Centre regional climate model projects changes in winter mean wind speed of a few percent over the UK. • Projected changes in storms are different in different climate models. Future changes in anticyclonic weather are equally unclear
Humidity	• Relative humidity decreases by around –9% (–20 to 0%) in summer in parts of southern England, but by less elsewhere. In winter, changes are a few percent or less everywhere.
Cloudiness	• Summer mean cloud amount decreases, by up to –18% (–33 to –2%) in parts of southern England (giving up to an extra +16 Wm-2 (–2 to +37 Wm-2) of downward shortwave radiation) but increase by up to +5% (zero to +11%) in parts of northern Scotland. Changes in cloud amount are small (–10 to +10%) in winter.
Sea level rise	• Relative sea level rise, with respect to 1990 levels, shows an increase of 36.3cm for London, 36.2cm for Cardiff, 24.4cm for Edinburgh and 25.3cm for Belfast under the central estimate.
Sea surface temperature	• Sea-surface temperatures around the UK coast have risen over the past three decades by about 0.7 °C.

In summary, by the 2080s, under the medium emissions scenario, average temperatures across all areas of the UK are expected to rise, more so in summer than in winter, and more so in southern England than in the Scottish Islands. The largest increases in precipitation are in winter on the western side of the UK. The greatest reductions in precipitation are in summer in the far south of

England. The wettest days in winter become wetter in England. Southern England sees the largest decline in summer wettest day rainfall. Relative humidity and cloudiness during the summer decrease in parts of southern England with minimal changes in winter and everywhere else. The UK Climate Projections do not include projections for changes in snow. However the Met Office Hadley Centre regional climate model projects reductions in winter mean snowfall of typically 65 to 80% over mountain areas and 80 to 95 % elsewhere (by the 2080s, relative to baseline climate).

Projections of future climate are different for other time periods and other emissions scenarios. For sea level rise a high++ (H++) scenario was developed to test vulnerability beyond the standard range of uncertainty included in UKCP09. The H++ scenario range indicates that time-mean sea-level rise around the UK could be 93 cm to approximately 190 cm in 2095 (relative to the present day mean of 1980–1999). Environment Agency advice[5] to organisations responsible for national infrastructure located at or near the coast is to plan for roughly 1 m of sea level rise by the end of the century, depending on location. However, they also indicate that caution is needed because sea level rise could be as much as 1.9 m over this time period.

3.3 Climate change at the global scale

Climate change is an international phenomenon. Across the globe, the evidence for climate change is uncontestable, with observed impacts on a wide range of natural and human systems. In their Fourth Assessment Report (2007), the IPCC set out a range of projections for global climate change and sea level rise. Since then, climate research has continued to develop, with climate models improving in skill and accuracy, and most recent projections indicate that without drastic cuts in emissions, global warming of 4 °C above pre-industrial levels could be possible by the 2070s (e.g., Betts et al., 2009)

Even if global efforts to reduce emissions succeed in keeping global warming to the 2 °C level, the impacts across the globe, and particularly in the already vulnerable and less developed parts of the world, are likely to be significant. For example, additional hundreds of millions of people are expected to be exposed to increased water stress in Africa, and freshwater availability in central and south-east Asia is projected to decrease. In high latitude regions, such as Siberia, rates of climate change are expected to be faster, and bring extensive impacts on permafrost stability. There are also likely to be impacts on human health, agriculture and food security, with climate change acting as a risk multiplier in parts of the world which are already challenged by a range of political and security risks.

In addition, sea level will continue to rise, leading to significant impacts on coastal populations, for example in Bangladesh. The heavily populated megadelta regions in Asia will be at greatest risk due to a combination of sea level rise, increasing flooding from the sea and in some cases from rivers. Aside from the direct impacts on populations in these areas, there is growing concern about the secondary social impacts arising as a result of migration, both internally and across borders.

The worldwide impacts of climate change are relevant for the UK's ICT sector because of our dependence upon international partners, suppliers, materials, and to some extent, skills and expertise. Wherever UK IT or telecommunications companies are reliant upon services, people or materials located elsewhere in the world, the potential climate risks in areas of concern should be considered as part of an overall climate risk assessment. We identify some of the major issues in Chapter 4.

[5] Presentation to transport authorities in the south east in the context of planning responses to the Adaptation Reporting Power, 5 March 2010. More detailed information, with reference to Defra's flood and coastal defence appraisal guidance available online at http://www.environment-agency.gov.uk/research/planning/116769.aspx.

4 Climate risks and opportunities for ICT

This chapter provides the assessment of climate risks and opportunities in the ICT sector itself. It draws heavily from the outcomes of the expert workshop held during the course of this project, amplified by case study material.

4.1 Identified impacts

4.1.1 Environmental standards for ICT components

Industry standards for the individual components which make up the ICT infrastructure include 'CE' certification and specific tolerances to, in particular, power supply, temperature and humidity. It is reasonable to say that the majority of devices typically used in the UK already have operating tolerances to temperature and humidity which will accommodate UKCP09 predicted temperature changes – both peak and average – provided they are appropriately installed and maintained.

Simple evidence for this is that the devices used in the UK are also used in a wide range of other countries which already regularly experience temperatures and humidity which fall outside the range of predictions for the UK. The same laptop computers, mobile phones, PDA's are used in both tropical and sub-temperate climates as are used in the UK. Ruggedised devices for use in harsh climates and for military applications also exist, showing that the technology is already available to address conditions more extreme than those predicted for the UK.

4.1.2 Climate impacts on ICT infrastructure

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. Table 4.1 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.

When the enabling infrastructure is considered, the challenge is rooted not in the devices themselves but in the environmental conditions which surround them and the impact of weather events. Vulnerabilities exist already, and 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, the bridge failure 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 again risk of water ingress and 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).

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 4.1 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 in only a few cases are the buildings in use actually purpose-built: 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.

Thus in some cases, there may already be significant expenditure on retrofitting and maintaining buildings for current uses and there is a chance that increasing demands of climate change may become too costly to address, forcing relocation perhaps.

Data Centres

A data centre is a facility used to install banks of computers 'servers' on which may be stored both 'applications' (programmes that do things) and 'data' (information used in those applications). These centres may be owned by and dedicated to a particular organisation (e.g., BT or Google) or may be 'shared', hosting applications and data for a number of separate users.

The commercial imperative that drives the ICT sector coupled to continuing development of applications and utilisation is leading to the commoditisation of a number of aspects of ICT, and the response is 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 the operation of the system relies absolutely on the availability of power and continuous data connectivity. This imparts significant vulnerability to the whole ICT system which, in the context of this report, is primarily connected with the physical location of the data centres and call centres.

These locations have the same vulnerability to climate change as any other above ground structure but have particular requirements which have to be considered. Their power consumption is massive both for operating the equipment and for cooling it and they tend to cluster around internet 'points of presence', i.e. they are co-located with high bandwidth, direct access to the web, increasing demand on the cabled (copper and fibre-optic) infrastructure. This clustering effect also causes a clustering of skills and expertise.

The economic and social impact of the failure of a data centre is potentially very high particularly as they carry much of the 'e-commerce' and 'EDI' traffic which enables the economy to function – including the collection of revenues and payment of benefits by government, which is increasingly handled through these locations. For example, the iDAQ data centre in Sheffield hosts the email server, website and intranet site for a global business providing residential care to around 2000 elderly and vulnerable adults. Information held at the centre may include full personal and contact information, treatment protocols, policies and procedures, patient records and treatment plans and so on. If this data centre (which is locally resilient) were to fail, or to become inaccessible via the ICT networks, the safety and well-being of these 2000 people in 7 countries and on 4 continents could be compromised.

Mitigation is available by ensuring that the vulnerability of existing data centres is addressed. The siting of future data centres needs to take into account the climate change risk 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. Power consumption is already recognised as a limiting factor on the location of data centres with some parts of the country already designated as 'full' from this perspective, e.g. Canary Wharf. As data centres are redeveloped to cope with climate change (both mitigation and adaptation) their power consumption characteristics will also change and this will need to be monitored.

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 is though subject to a different set of climate change impacts and can be affected by climate change in a number of 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.

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, in practice, 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.

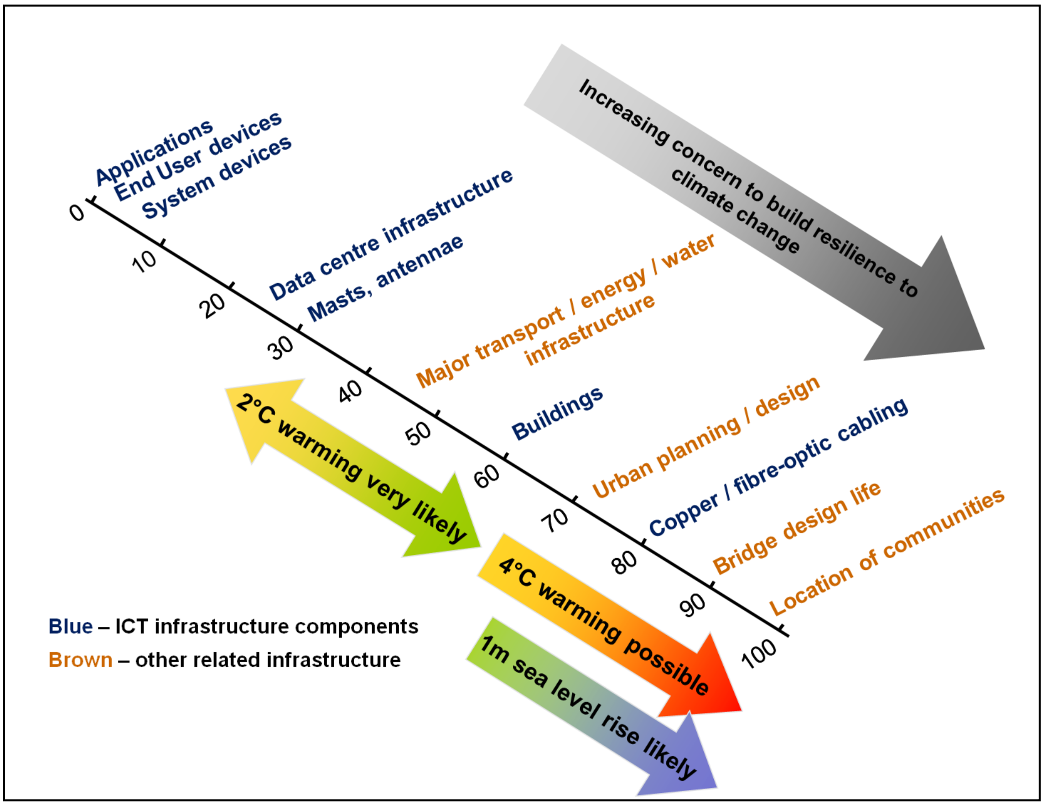
4.1.3 Lifetimes of infrastructure

While Table 4.1 shows that there are a wide variety of ways in which weather can affect ICT infrastructure, understanding the scale of the impact of climate change necessarily brings into question the lifetime of individual 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. It is to be expected therefore that up until the 2030s many of the buildings and masts will be the same – but the devices they accommodate may be refreshed 4 or even 5 times. That said, because of their size and/or complexity, some devices being built in to data centres are expected to have the same lifetime as the centre itself (20-25 years).

Figure 4.1 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. Thus, the 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 provide the sector with 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 4.1 Lifetimes (in years) of ICT infrastructure components compared with illustrative climate change timescales


0
10
20
30
40
50
60
70
80
90
100
Applications
End User devices
System devices
Data centre infrastructure
Masts, antennae
Major transport / energy / water infrastructure
Buildings
Urban planning / design
Copper / fibre-optic cabling
Bridge design life
Location of communities
Increasing concern to build resilience to climate change
2°C warming very likely
4°C warming possible
1m sea level rise likely
Blue – ICT infrastructure components
Brown – other related infrastructure

4.1.4 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. For example, a religious order operating care homes in 4 continents and 7 countries has a single website hosted at a data centre in the UK which also hosts their global email system and intranet applications. The 'care' application is hosted at a different location in the UK and is used by homes in 2 of the 7 countries. The functionality of the care homes overseas is reliant upon the UK and international infrastructures. This functional architecture is adopted by many organizations and is enabled by the 'speed of light' data transmission capability of the fibre-optic network. There is then a substantial 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. Telegraph poles are sourced from high-latitude countries and their continued availability may be threatened by climate change whilst rare and precious metals may be subject to both political and the operation of market forces – probably increasing prices. 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. Increasing carbon-fuel prices driven by shortages, changing taxation and carbon reduction programmes will also increase the costs of shipment. While availability may be maintained, costs may become unsustainable.

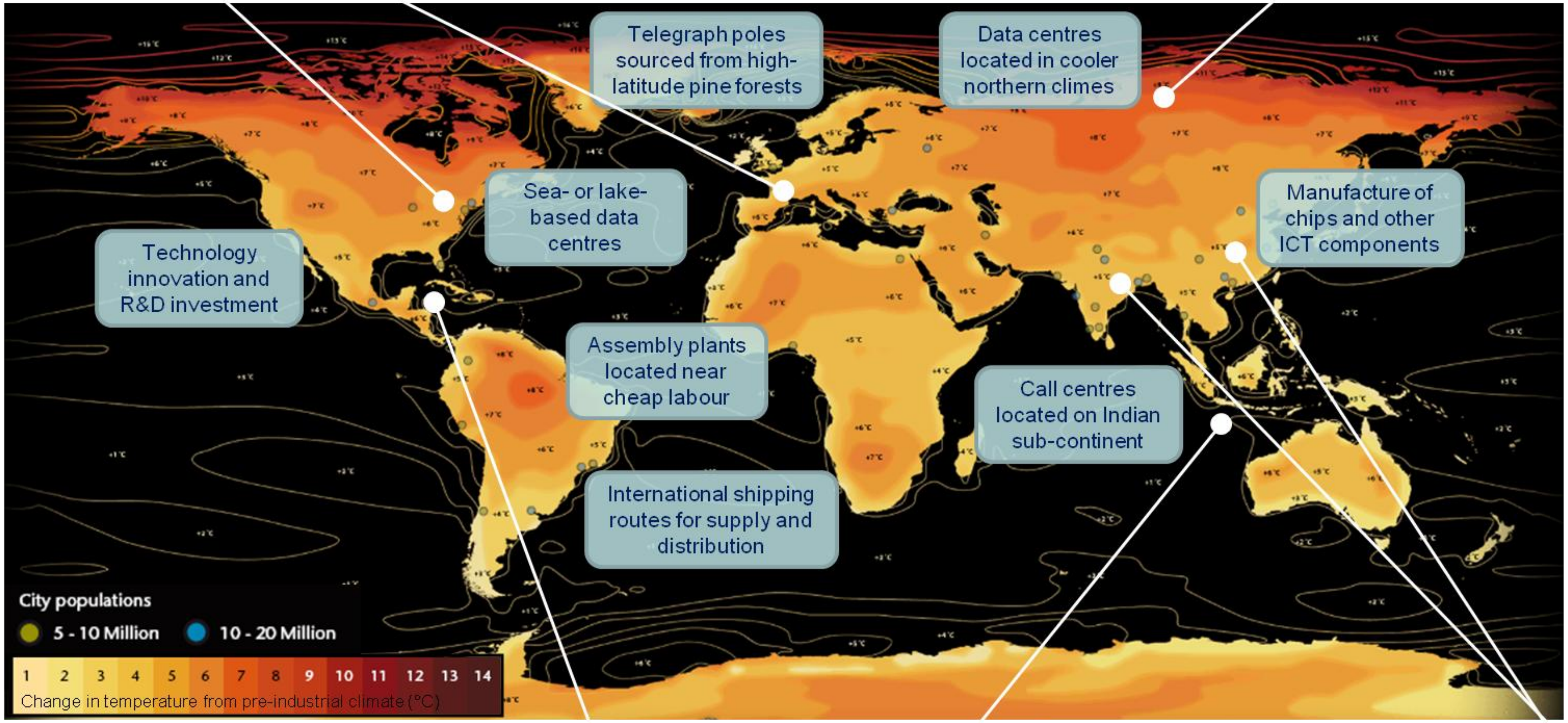
Rising sea levels and extreme weather events will also affect the operation of data centres and service centres in low lying areas such as the Netherlands and vulnerable areas of the sub-continent of India. The full risk associated with 'off-shoring' of data, service and call centres needs to be evaluated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

Figure 4.2 illustrates some of the ways in which climate change around the world may affect ICT in the UK.

Figure 4.2 **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)

Hottest days of the year could become as much as 10-12 °C warmer over eastern North America; as much as 8 °C warmer across Europe.

Almost complete disappearance of near-surface permafrost from Northern Siberia. Reduction of permafrost in Canada and Alaska. Infrastructure built on permafrost foundation at risk.


Telegraph poles sourced from high-latitude pine forests
Data centres located in cooler northern climes
Sea- or lake-based data centres
Manufacture of chips and other ICT components
Technology innovation and R&D investment
Assembly plants located near cheap labour
Call centres located on Indian sub-continent
International shipping routes for supply and distribution
City populations
● 5 - 10 Million
● 10 - 20 Million
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Change in temperature from pre-industrial climate (°C)

Sea levels could rise as much as 80 cm by the end of the century, and by much more in the longer term. Increases are greater at low latitudes, affecting low-lying regions like Bangladesh, Indian Ocean coast and south-east Asian coast.

Tropical cyclones could be more intense and destructive. Global population increases in coastal areas and SLR mean greater cyclone and hurricane-related losses, disruption to infrastructure and loss of life as a result of storm-surges.

Rice and soy-bean yields could decrease in all regions of production including China, India, and the Americas. Water resources from glacial melt could reduce significantly in Indus river basin and western China. Increasing food and water security concerns for affected populations.

Both within the UK and internationally there is a threat arising from the incidence of extreme weather events which (as evidenced by the UK snow in January 2010) can 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 from home or otherwise 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 is likely to become a tradeable commodity at an international level, impacting availability, cost and resilience.

Long-term resilience in ICT will draw upon investment in the research and development of future technologies to generate innovations capable of dealing with the challenges arising from climate change and the different patterns and types of use that will develop. 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

4.2 Consequences of climate impacts

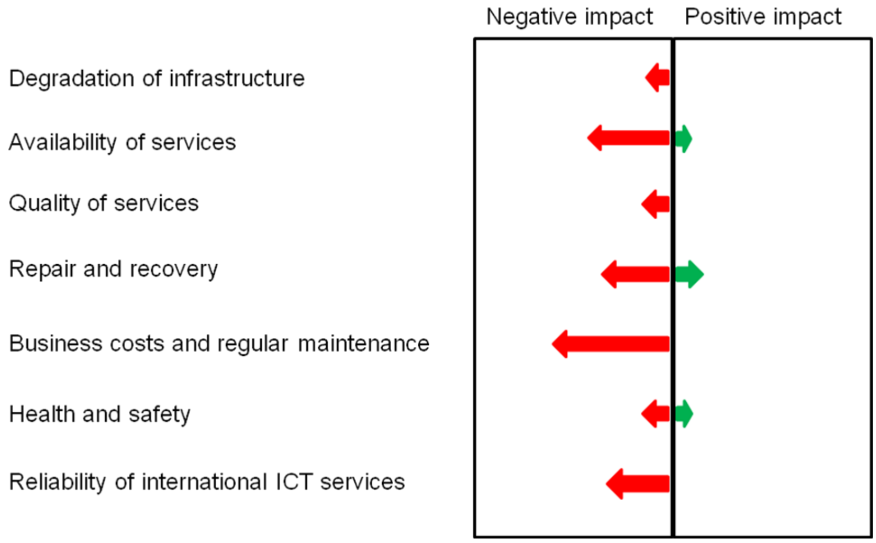
Climate change may impact on the ICT sector in a wide variety of ways, as indicated in Table 4.1. However the consequences of these impacts, alone, or in combination, can be reduced to a smaller number of key issues:

- 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

To this list, we can also add a further consequence from the consideration of supply chains and the international climate change context: changes to reliability of international ICT services.

Table 4.1 also gave an indication of whether the consequences of climate impacts would 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 4.3.

Figure 4.3 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 reducing likelihood of snowfall, with all its implications for damage to infrastructure (snow-loading) and disruption to maintenance and repair schedules. Additionally, this will mean that engineers are 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.
- Given that the responsibility for dealing with climate risks to privately-owned ICT lies with the end-user, there is a role, and a potential business opportunity, for a knowledgeable ICT sector to educate customers about climate change impacts.

With reference back to Table 4.1, it is also important to note the anticipated level, or geographic scale, of the consequences of climate impacts. 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.

The majority of impacts are likely to cause disruption at the level of individual organisations (both providers and users of ICT services, such as BT or the East Coast Mainline Company), or local geographical areas (such as Morpeth in 2008, or Workington in 2009) 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". However, 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 2010[6].

[6] 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

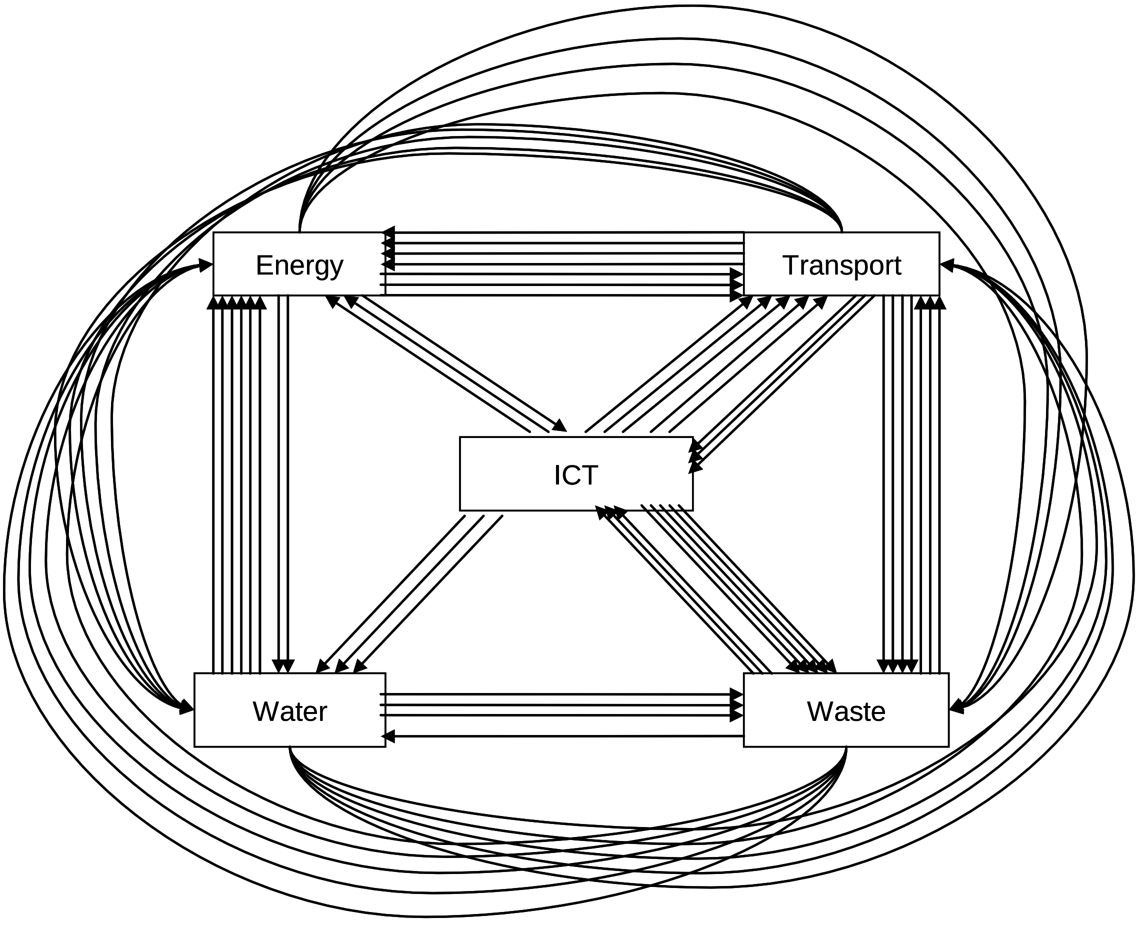
5 Cross-sectoral implications

Chapter 4 considered climate risks to the ICT sector itself. In this chapter, we assess the ways in which climate change may exacerbate the risks faced by other national infrastructure sectors, and business in general, as a result of their dependence on ICT. We also consider (more briefly) the ways in which climate risks in other sectors can knock-on to the ICT sector.

5.1 Review of critical interdependencies

A recent report 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 (AEA, 2009a). Figure 5.1 illustrates these relationships.

Figure 5.1 Critical interdependencies in national infrastructure



Detailing these 15 inter-dependencies, the prior work found that whilst the ICT sector is predominantly dependent on the provision of energy, each other sector is dependent on ICT for its continued daily operation. Remembering the definition of ICT as including both voice and data communications, there is not considered to be a single business in the UK which does not depend on telephone communication (though there are undoubtedly some individuals in that position) whilst increasingly, 'business as usual' for all the other sectors depends on their ability to communicate with people and devices via data or voice links.

Transport	depends on	ICT	5
Energy	depends on	ICT	2
Water	depends on	ICT	3
Waste	depends on	ICT	5

Resilience in the ICT systems as a whole is therefore critical to the continued operation of the other sectors. These dependencies are identified in Table 5.1.

Table 5.1 Critical dependencies on ICT

The nature of critical dependencies upon ICT	
Category	Dependence upon ICT
Business as usual	Customer transactions (including electronic banking) Staff to staff communication (email, phone call, video-conferencing) Financial management E-commerce Ticketing and billing systems Customer/passenger information systems Healthcare provision ATMs
Control Systems	Traffic Signalling Traffic Management Navigation (water borne, satellite and land-based) Vehicles – road and rail Aircraft and Marine Vessels Rail Signalling Air Traffic Management Supply-chain Management Logistics (goods despatch and delivery) Real-time delivery management and reporting SCADA Remote management of pumps and switches in network Water distribution Energy generation and distribution (especially nuclear and ‘smart grid’) ICT network management (much of the infrastructure is managed through the infrastructure!)
Incident Management	Policing, Fire & Rescue, Ambulance (esp Airwave) Transport delay rectification Natural emergencies (e.g. Cockermouth) Man-made emergencies (e.g. Buncefield)

These systems, and many others, are so embedded in the operation of businesses and our daily lives and so reliable that we are hardly aware of their existence. We only notice them when they do not function as we expect – but they are completely integral. As was seen with the impact of Hurricane Katrina on New Orleans, the shift from post-industrial society to chaos through the failure of these systems is measured in the space of a few hours.

The CST clearly identifies key factors within the National Infrastructure in terms of its highly interconnected nature and fragmentation of delivery and governance which mean:

- “No-one has any responsibility or accountability for looking across the NI as a whole i.e. across the network of networks”
- “There is little or no knowledge of vulnerabilities and risk arising from interdependencies across the NI which means that investment in adequate resilience will always be low priority”
- “Little or no expenditure occurs on a precautionary basis, instead the approach is to perform heroic acts in times of crisis”
- “Despite significant levels of investment by the private sector in recent years, they do not believe market forces by themselves will deliver a resilient NI fit for the 21st century”

5.2 Climate implications for NI sectors

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).

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, leading rapidly to a major problem on an infrastructure sector which can be considered close to capacity under ‘business as usual’ conditions.

Other systems will, of necessity, default to safe; that is they will shut down, in the event of system failure or outage. Power generation, particularly nuclear, requires multiple communication systems to be ‘in synch’ at all times in order for the plant to operate safely, if these conditions are not met, the plant will failsafe

A significant failure of elements of the ICT in any one geographic region will 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 would 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.

Unknown and unmitigated risk of consequential failure of other elements of the infrastructure exists throughout the ICT system. Reference to the ITIL standards and norms reassures that for ‘normal’ conditions the sustainability of service is very high with guaranteed availabilities of around 99.97% or thereabouts - a 1 in 10000 risk of failure on any given day. From the perspective of a commercial ICT provider the cost of further reducing the risk is greater than the benefit a typical client is willing to pay for and service contracts would typically exclude force majeure under which category extreme weather events and consequential business risk could be considered to fall.

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 as managing demand and capacity (in all elements of the infrastructure) becomes more economically and environmentally sustainable than increasing it.

This will also require more intensive and intelligent management and use of data for forecasting and managing demand (for energy and other things) – especially in relation to weather events, dissemination of information to different classes of user and to support developments in design of information systems.

5.3 Climate implications for business

The statistics provided in Table 2.1 highlighted the extent to which “UK plc” is already reliant on the effective functioning of the ICT sector: 98% of business reliant on ICT, 90% of high street purchases using plastic cards, £50 billion online spending, 4.2 million working flexibly, 1 million directly employed in the sector. Comparing these statistics with the unrealised potential of current ICT, there is substantial scope for growth in these numbers. As generational shift occurs, this growth will be increasingly realised and the reliance on ICT will increase at least in proportion. Equally, wider more effective application of the ICT to all forms of work will further increase the demand.

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.

As an example, the Low Carbon Transition is likely to lead to demand for a change in working patterns. While there is already a well-established shift to home-working and remote working (relying on both broadband and mobile telephony systems), the pace and extent of this shift is likely to increase over time as government, employers and employees begin to understand and seek to achieve the benefits of the change. These might include, for example:

- reduced numbers of commuters (road and rail)
- reduction in demand (or reduction in growth of demand) for commuter travel
- lower demand for growth in new transport infrastructure
- less intensive use of existing infrastructure
- smaller, more intensively used, office buildings (lowering capital requirements as well as energy consumption)
- potential increases in labour productivity (2+ hours per day released from travelling may, at least partly, be devoted to working)
- less disruption of work due to extreme weather events – employees not commuting become less vulnerable to travel disruption so that flood, snow and extreme heat are less disruptive to the economy than is currently perceived to be the case.

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. Whilst many homes currently have multiple access (broadband or adsl, landline and mobile) and receive a very high level of service reliability there is an acceptance that one or more of these might fail temporarily. As reliance on these services increases, consumers will need to be willing to pay for more resilient solutions[7] and both additional lines and bandwidth.

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. They may also need to invest in learning to work and manage. Resilience of ICT in these circumstances may require that the sort of business continuity and disaster recovery plans that are currently put in

[7] Such solutions might include, for example, use of ‘3G dongles’ to guarantee internet access when landlines are lost – this provides internet access via the mobile telephone network.

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. This might require a shift in the pricing and business models for both providers and users. It could even lead to reconsidering the resilience of the system beyond the conventional point and extending it to the level of the individual user – for example by providing multiple, separately routed, lines into domestic premises – something which is very rare at present.

6 Adaptation in the ICT sector

In this chapter, we explore the options available to mitigate the climate risks identified in this study. The chapter also considers some of the challenges and barriers to adaptation in the ICT sector.

As discussed in previous chapters, it is important to recognise that (particularly 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 therefore 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 a 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.

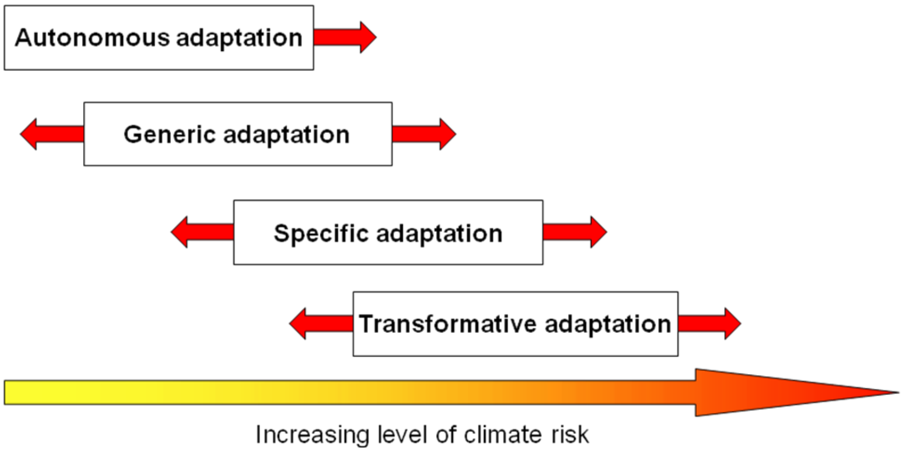
The increasing dependence in coming decades of infrastructure, economy and society on ICT, plus the likely increases in the kinds of weather events which can already disrupt ICT, mean that from the perspective of those organisations which use and provide services it will become increasingly important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

This section therefore explores the adaptation options available to mitigate some of the local challenges of climate change on ICT.

6.1 Categories of adaptation

Jones et al. (2007) identified that different kinds of adaptation response are appropriate depending upon the scale of climate risk to be managed. Each group is assumed to be more difficult to implement than the previous, but provides a more substantial level of risk management. The four categories are shown in Figure 6.1.

Figure 6.1 Categories of adaptation appropriate for different levels of risk (after Jones et al., 2007)



- *Autonomous adaptation* refers to those reactive responses that occur on the basis of experience, and probably without any deliberate concern to address potential climate change impacts.

- *Generic adaptation* includes all of those capacity building activities which can take place irrespective of context-specific needs, such as improved access to technology and information, wealth creation, increased social capital, institutional reform, etc. These are comparatively easy to undertake, generally inexpensive and have a number of co-benefits.
- *Specific adaptation* refers to those options implemented to manage particular climate risks identified within a specific context. They include things like new technologies, retrofitting existing structures, disaster planning, etc and may also require further investment in research and development. Specific adaptation extends or evolves 'business as usual'.
- *Transformative adaptation*, by contrast, is more substantial, and may involve abandoning or replacing whole business activities, or transforming them; it is likely to involve new technologies, new paradigms or both.

In relation to building climate resilience in the ICT sector, there appear to be possible responses ranging from autonomous right through to transformative adaptation. 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. There are various specific adaptations in which resilience to weather impacts may be enhanced, and some of these are discussed further in the following section. These include awareness-raising, research and development, planning, contingency planning, adapted procedures, etc. Many of these improvements in climate resilience frequently offer additional benefits (cost savings, improved efficiency, resource efficiency, etc).

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.

It is also useful to consider adaptation options across the four conventional action categories for risks mitigation. These are described in Table 6.1.

Table 6.1 Possible actions to mitigate risk

Conventional risk mitigation options	
Action category	Description
Accept	An informed decision to accept the consequence and likelihood of a particular risk (a "do nothing" option, usually accompanied by contingency or response plans)
Transfer	Shifting the responsibility or burden for the loss occurring if the risk is manifest to another party (typically through supply chains or insurance)
Reduce	Selective application of specific actions to reduce either the consequence or the likelihood of a risk.
Avoid	An informed decision to change systems, procedures or policies so as to step out of, or prevent, the risk situation.

Similarly, the recently published Sector Resilience Plans emphasise the importance of different types of responses to improve resilience generally (Cabinet Office, 2010b):

- Reduced vulnerability (e.g. through permanent or temporary measures)
- Improved preparedness (e.g. through early warnings, contingency planning, cooperation)
- Improved response/business continuity measures (e.g., adopting business continuity standards)
- Improved recovery measures

In ICT, as elsewhere, adaptation actions to address climate risks will rarely (if ever) be undertaken as a response to climate change alone. Rather, a combination of factors more usually leads to adaptation. In this instance, given the backdrop of resilience and flexibility within the ICT sector as a whole, it is those options which provide clear additional benefits that will be most likely to be adopted.

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.

(Some form of economic appraisal of the full range of costs and benefits associated with taking action or doing nothing can help in this regard.) In the section that follows, we identify areas of adaptation to enhance climate resilience to a range of natural hazards now, to take advantage of technology developments, and to improve current responses to weather events.

6.2 Adaptation options for ICT

We have identified five main areas for adaptation to the impacts of climate change:

- 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

There is a wide range of potential climate risks identified (see Table 4.1), and the specific adaptation actions appropriate in each individual circumstance would need more detailed analysis in the context of local infrastructure, service requirements, and customer relationships. 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.

6.2.1 Enhancing climate resilience of the network

While we have already noted the inherent resilience available in the multiple networks which make up ICT, there are nevertheless ways in which this resilience 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.

While urban areas are well-served by a wide range of alternative network coverage, more rural and potentially more vulnerable locations (such as those at the end of network lines, those which have access to only one mobile network and those which can be difficult to access during times of flood) do not have the same level of service. 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, which may or may not be in line with ‘commercial decision’ standards. 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.

6.2.1 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, the example of the combination of climate change and the drive towards free-air cooling in data centres (see case study in Chapter 7) shows that in some instances there may be a commercial interest in developing devices and components with higher temperature operating ranges. In the data centres context, the R&D is driven by the need to reduce energy and water consumption for cooling, but additionally, the technological advance will provide adaptation to climate change. 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.

In relation to devices, there seems to be no requirement to change technical standards or product specifications as a precautionary response to climate change. In most cases the product life is far too short to warrant a specific consideration of climate change in its lifetime. Instead, product design (and accompanying standards) is expected to ‘evolve’ over time, in response to a range of driving factors, one of which could be experience of weather events.

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 pieces to be integrated into the infrastructure. One other recent advance in technology which is suited to adaptation is the trend towards reprogrammable technologies, or so-called “chameleon” devices, which could enable a range of different functions, each tuned to suit the particular environmental conditions encountered during a product’s life.

6.2.2 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. This kind of strategy has already been proposed in relation to Google’s free-air cooled data centres, but it could also be driven by warnings of other weather events. This approach requires some level of redundancy within server networks (and so may come at some additional cost) and is also going to be more widely available to large organisations than SMEs.

6.2.3 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, just as in any other sector. 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. In order to facilitate this kind of planning, there may be a need for mapping and access to relevant data.

It may be possible to tune other business processes to drive a market for increased climate resilience of services provided. Procurement and contractual processes, particularly those used by large companies, 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” this additional resilience. In this situation, there might be some 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 / procedures 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 (e.g. BS 25999[8]) by both providers and consumers of ICT will help, though it may need specific consideration by each individual organisation of how current business continuity plans sit in the context of climate change.

6.2.4 Improving responses to weather events

The telecommunications providers are already well equipped to respond to the consequences of environmental disruption to networks. However, the general approach to dealing with 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 a potential for increasingly severe and frequent weather disruptions, an “accept and respond” approach may become increasingly expensive, and unsatisfactory from a customer perspective.

[8] Available from the BSI Group at http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999/

Nevertheless, there are a number of ways in which 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 or which providers have had little past experience of. Responses could be improved through the 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). Better collaboration with local authorities may help to ensure a more efficient and effective recovery phase following weather disruption.

6.3 Challenges and barriers

The study has identified five main challenges or barriers to adaptation:

- Climate change risk awareness and action in the private sector
- Current business model for resilience
- Business case for action on climate risk
- Ownership and sharing
- Scale effects

6.3.1 Climate change risk awareness and action in the private sector

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. This study reviewed the responses of telecommunications companies to questions about climate risk in the Carbon Disclosure Project (2009), and this revealed that telecommunications providers are now starting to become “climate risk aware” (see Appendix 4). Some are considering the issues in the context of contingency planning, and some are beginning to develop adaptation strategies. However, there is still a need for much greater awareness of climate risks across all of the key organisations responsible for ICT infrastructure.

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 (e.g., failures in the energy sector that affect the ICT sector, extreme weather impacts on road that affect maintenance and repair of telecommunications infrastructure). Underlying trends towards a highly-digitised and interconnected world will need systems thinking to manage climate, and other, risks effectively. Climate risk will need to be analysed and managed throughout service supply chains. There is a role for a knowledgeable ICT sector to educate the customer about the potential risks and opportunities that a changing climate might present.

6.3.2 Current business model for resilience

It has been established that the ICT infrastructure is designed and built to offer an already high level of resilience simply to ensure effective operation under business as usual conditions. It copes with the normal spread of weather events, natural and unnatural disasters and the varying competence of users in a robust manner. All of this is driven by the underpinning business model of ‘user pays’ – and of course the user won’t pay if the ICT system is not available.

Some of the limits to climate resilience are rooted in that same business model. The customer will only pay for so much resilience – and the cost of increasing beyond that level rises disproportionately to the resilience gain made. A ‘commercial’ decision is then being taken and as far as possible ‘conditions beyond our control’ is the get out clause for service failure. Providers trade off the revenue lost from a service outage against the cost of its prevention – the balance of those two factors 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.

There is therefore a limit to the amount of resilience that owners will provide and, for normal purposes, that is acceptable. They design and build equipment and systems to accommodate the range of climate conditions that have historically been considered ‘normal’ (and even then as has been seen through the 2009/10 winter, the system can fail).

One step towards improving specifically climate resilience will be the education of system designers to understand the future range of climate conditions – in particular the frequency of those conditions – which will then shift the balance of investment towards a more resilient system. For this to be achieved without regulatory intervention, they will have to be convinced by solid evidence of the increased likelihood, severity and frequency of extreme weather events. These factors will then be built into their investment models and the additional resilience provided as a function of commercial risk reduction.

6.3.3 Business case for action on climate risk

With regard to the specific above ground elements of the infrastructure such as masts, switching stations, exchanges, data centres and so on, these are vulnerable to risks in relation to flooding, subsidence, precipitation and heat. However 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 sector.

This study could not find any research either in the UK or elsewhere in the world which has modelled the scale and cost of future events, either on ICT infrastructure or in the sector more widely. There is therefore an underdeveloped "business case" for providers (and customers) to invest in enhanced climate resilience, and this is a considerable barrier to adaptation.

Improving climate resilience of infrastructure elements will be a function of convincing evidence that they are likely to be sufficiently threatened as to make investment worthwhile, but this will also need to be examined from a planning consent perspective. There is a balance in this regard: the infrastructure elements tend to be constructed where greatest demand is located, and so the infrastructure follows the change in the built environment, meaning that co-location of infrastructure with homes, offices and factories is important from an effectiveness and utilisation perspective.

There is probably a need therefore to look at these matters from a local planning perspective, considering risk to the built environment and ICT infrastructure through the lens of climate change predictions to ensure that critical elements of the infrastructure are not developed in locations likely to be vulnerable to extreme weather events and, if they do need to be developed in those locations, that they adopt design standards and performance tolerances capable of dealing with the predicted events. It doesn't matter if a mobile phone base station is exposed to high winds if it has been designed and built to operate under those conditions – and it is easier to solve that problem than it is to obviate the high winds.

6.3.4 Ownership and sharing

A recent study highlighted a significant barrier to building resilience in general in the ICT sector in that "individuals and most businesses are not concerned with the infrastructure itself – we simply use it. Telecommunications businesses are primarily concerned with capacity and bandwidth issues for 'business as usual' and the prime role of the regulators (where the services are regulated at all and much of the ICT industry is not) is concerned with licence pricing, bandwidth allocation and competition," (AEA, 2009a).

The Universal Service Obligation[9] (USO) in telecommunications (part of the Communications Act 2003), does include the underlying principle that services which are used by a majority and are therefore necessary to maintain social cohesion, should be universally available and at an affordable price. Ofcom has designated BT and Kingston Communications (in the Hull area) as the Universal Service Providers in the UK.

Commercially, there is an increasing 'sharing' of elements of the infrastructure. For example, BT, Cable & Wireless, Virgin Media and others lay underground cables to support data and voice transmission. The 'market' in this area is largely at the level of service provision with most suppliers selling a 'service' based on rebundling bandwidth that they have purchased from the primary infrastructure providers. This sharing needs to become fully transparent to service users such that

[9] The USO guarantees that everyone can make and receive local, national and international calls, faxes and data communications from a fixed location, while also ensuring that a sufficient number of payphones are available in public areas. These services must be made available at a specified quality to all end-users in the territory, regardless of their geographical location. The USO also requires that everyone must be able to access publicly available telephone services such as directory enquiries, operator assistance an emergency services and that suitably adapted telephone services are available for end-users with disabilities.

they understand their risk and exposure. By gaining such understanding they are more likely to take individual mitigation action and spread their risks.

In practice, any assured provision of reliable and uninterrupted ICT services to the wide range of users who depend upon them arises from the combined (though not necessarily coordinated) efforts of individual consumers, private sector suppliers and statutory bodies.

6.3.5 Scale effects

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 large nondescript data centre which may have little connection with local communities and yet be of great national importance. Other technological advances could prove to be an even greater challenge to this approach as data and applications critical to national functioning start to be located outside the UK or in areas under international jurisdiction (such as plans articulated my Microsoft and Google).

The study has also uncovered the potential for equity issues related to the impacts of climate change in the ICT sector. Rural single-sited SMEs are potentially more vulnerable to localised weather-related disruption of their ICT than larger multinational companies. Larger companies also have a greater capacity to transfer their ICT requirements between sites around the world to avoid weather risks. Adaptation presents a greater challenge to SMEs, both providers and users of ICT.

6.3.6 Additional barriers

A number of other barriers to adaptation in the sector were identified during the study. These are summarised in Table 6.2.

Table 6.2 Additional barriers to adapting the ICT sector to the impacts of climate change

Some barriers to building climate resilience	
Information and data	Timescales
• Greater certainty in likelihood and impact of climate risks is needed • Working with uncertainty: need more evidence of impacts to make the business case for new or different designs • More detailed data is needed to enable changes in design	• Investment cycles, strategic planning timeframes and political timeframes on election cycles are all too short to enable long term planning for climate change
Common standards	Cost and Market
• How to differentiate between systems offering more/less resilience: evaluation criteria or common standards may be required, but need better understanding of risks to identify these • Design for a wider range of futures is difficult	• How do you get people to pay more for greater resilience? Customer demand/willingness to pay *vs* brand impact • Competition may inhibit data sharing across companies for the common good • Regulator currently emphasises economic aspects, and has little power in relation to resilience • Greater resilience will cost more

7 Case Studies

This chapter presents three case studies explored during the course of the project. The first two (Cockermouth and Data Centres) look at potential climate risks and opportunities using data from the UK Climate Projections (UKCP09), while the third highlights interdependencies between rail and ICT in the context of climate impacts.

7.1 Case study: Flood impacts in Cockermouth, 2009

In November 2009, flooding occurred across North Wales, Cumbria and the Scottish Borders. Extreme rainfall totals were recorded with a record-breaking total rainfall of 314 mm falling in one 24-hour period in Seathwaite, Cumbria (CEH, 2009). The amount of rain typically expected in the west Cumbria area during the entire month of November had fallen in 24 hours. The rainfall caused widespread flooding in Cumbria particularly around Cockermouth, Keswick, Workington, Kendal and Ulverston. The events reemphasised just how vulnerable the UK's critical infrastructure is in the face of extreme conditions. The failure of a single piece of infrastructure, such as a bridge, not only causes difficulties in reaching basic commodities and local services, but also leads to the failure of other connected infrastructure networks, such as electricity, gas, telephone lines, waste and water supply.

In Cockermouth, where water levels reached 2.5 m above normal, more than 200 people were rescued by emergency services, 50 of them by RAF helicopters (BBC News, 2009). Alongside the immediate human and social disruption caused by the event, major infrastructure was also badly affected with 6 bridges lost in the Cumbria area, and more than 1800 requiring inspection for damage and safety Local and trunk roads were closed, phone lines were lost and electricity was disconnected.

7.1.1 Consequences of the 2009 flood event for telecommunications

The flooding and bridge collapse disconnected 2500 telephone lines in Workington, 700 in Cockermouth and a further 300 in North Cumbria, around 3500 in total. In addition, 5 Airwave base stations (emergency communications stations) were affected, of which 2 were still not functioning 5 days after the event[10]. Whilst BT formed an engineering task force to reconnect homes as rapidly as possible, temporary mobile base stations were installed to mitigate the losses to the airwaves system. The copper cables carried by the collapsed Calva Bridge took around 7 days to restore with engineers routing a cable beneath the river bed, this being the fastest way to restore service, and arguably a more resilient long term solution. Restoration of energy supply to over 1200 homes, without which much of the ICT cannot function, took about 9 days.

The impact of an event such as this in a much more heavily populated area could be much more extensive as it could have the potential to knock out numerous network points potentially affecting re-routing.

7.1.2 Flood events and climate change

There are inevitably concerns that a devastating flood such as this one occurred as a result of climate change. While no single flood event can be directly attributed to climate change, in general, climate change is expected to intensify the hydrological cycle. It is also expected to lead to increased rainfall in winter, and to increased rainfall extremes, which may cause flooding.

England's North West has become wetter in the recent past. Winter rainfall has increased in this region since the early 1960s. Extreme rainfalls have also increased in frequency in northern and western areas of the UK, and one recent CEH study found that, over the last 50 years, daily maximum rainfall has increased by 25 % in these areas, relative to the previous 50 years. UKCP09 projects increases in winter rainfall for the future in these areas, and there are concerns that extreme rainfall will become more common in future. In this context, it can be said that extreme rainfalls are consistent with a tendency towards the North West becoming wetter and more extreme in future.

[10] However, due to the inherent resilience in the design of the Airwave system, Airwave availability was at no point affected by this loss.

7.1.3 Results from the UKCP09 Weather Generator

We used the UKCP09 weather generator to explore how precipitation patterns (and by implication, flooding) in this area are expected to change in future. We investigated how the intensity of wet days may change under the high emissions scenario in Cockermouth. We used only the high emissions scenario to provide an indication of the most extreme case available in the dataset. A wet day is defined as a day with more than 10 mm of precipitation. We defined a "wet day intensity index" as the total amount of rain falling on wet days divided by the number of wet days in the year. We used the Climate Projections to investigate changes in the wettest day and the most extreme precipitation on the wettest day in a season.

Baseline climate (1961-1990)

- The **daily wet day intensity index** for Cockermouth in the 1961-1990 **baseline** is **6.3** (an annual wet day rainfall or snow total of 200mm divided by 32 wet days).
- **19%** of **annual rainfall or snow falls on wet days in winter** where daily precipitation is over 10mm per day.
- There is no change on the wettest day for the 1961-1990 baseline in Cockermouth.

2030s (high emissions scenario)

- The **daily wet day intensity index** for Cockermouth for the **2030s** is **7.1** (an annual wet day rainfall or snow total of 244mm divided by 35 wet days).
- **23%** of **annual rainfall or snow falls on wet days in winter** where daily precipitation is over 10mm per day.
- In Cockermouth, there is a **90% likelihood** that **precipitation on the wettest day** in **winter** will be, up to and including, **21% greater** in the 2030s.

2050s (high emissions scenario)

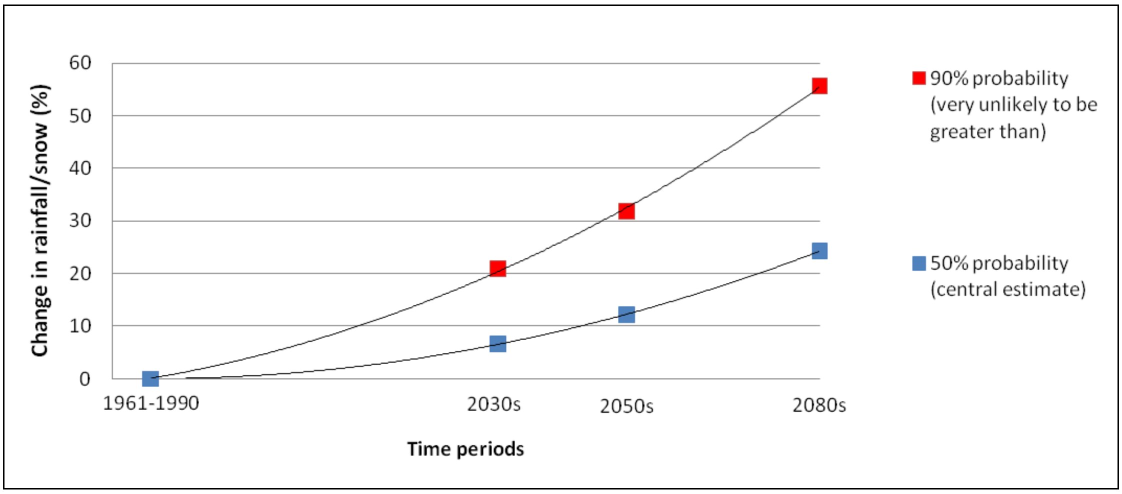
- The **daily wet day intensity index** for Cockermouth for the **2050s** is **7.5** (an annual wet day rainfall or snow total of 273mm divided by 37 wet days).
- **25%** of **annual rainfall or snow falls on wet days in winter** where daily precipitation is over 10mm per day.
- In Cockermouth, there is a **90% likelihood** that **precipitation on the wettest day** in **winter** will be, up to and including, **32% greater** in the 2050s.

2080s (high emissions scenario)

- The **daily wet day intensity index** for Cockermouth for the **2080s** is **8.2** (an annual wet day rainfall or snow total of 327mm divided by 40 wet days).
- **29%** of **annual rainfall or snow falls on wet days in winter** where daily precipitation is over 10mm per day.
- In Cockermouth, there is a **90% likelihood** that **precipitation on the wettest day** in **winter** will be, up to and including, **56% greater** in the 2050s.

Figure 7.1 illustrates the change in the amount of precipitation falling on the wettest day in winter projected for Cockermouth, under the high emissions scenario.

Figure 7.1 Results from the UKCP09 projections over land for Cockermouth (grid square 9999), showing the percentage change in precipitation falling on the wettest day in winter (high emissions scenario)



7.1.4 Conclusions for flood resilience

Even by the 2020s, an increase in the amount of precipitation on the wettest day is projected. The intensity of wet days increases throughout the century. By the 2050s, the amount of precipitation on this wettest day has increased by up to 32 % and by up to 56 % for the 2080s, compared to the baseline of 1961-1990. While the 2009 event was unprecedented (and the maximum amount of rain falling on a single day in any of the weather generator results across all time periods did not exceed 110 mm), all of the trends support the view that climate change will bring more severe extreme weather. Improvements in the resilience of telecommunications infrastructure to these and similar weather-related disruptions, in order to avoid interruptions to ICT services, may be increasingly warranted in future.

7.2 Case study: Temperature and humidity impacts on data centres

7.2.1 Introduction

Data centres house computer systems, server and network infrastructure and associated storage platforms. Many organisations operate their own data centres in house. However, as the role of computer systems and network services becomes ever more critical to the success and growth of the economy, many organisations are looking to third party providers to support their expanding data centre requirements. Data centre operators can provide highly secure and resilient environments for the outsourcing of all or part of the hosting and management of organizations technical, web and IT infrastructure to ensure these systems remain ‘always-on’. Outsourced data centres come in all shapes and sizes. They range from carrier owned – such as those operated by BT, to so-called ‘carrier-neutral’ – such as those operated by UK-based European data centre specialists such as TelecityGroup. Typically, carrier-owned data centres are built to house the servers and networks of the carrier, or network-provider’s equipment and those of its customers. Carrier-neutral data centres usually offer access to a much wider range of connectivity providers, all of which have built their networks into the data centre thus creating Internet ‘hubs’; physical locations where network operators and ISPs can exchange traffic with each other and with content providers and other organisations whose systems are also hosted in the data centre. These types of data centres differ from the in-house, proprietary data centres in being able to offer much higher levels of connectivity, and are home to a significant proportion of the UK’s most online-intensive organisations – both Government and enterprise (DCMS and BIS, 2009).

Data Centres are governed via a European Code of Conduct which includes guidelines, recommendations and an inventory of good practices that could reduce energy usage by up to 20%

(JRC, 2010). The best practice document sets out a number of simple measures that can reduce energy usage by data centres. These include the creation of "virtual servers", the reduction of overcooling and the use of natural cooling. The Code includes best practice guidelines on Resilience Level and Provisioning, Temperature and Humidity Settings ,and Free and Economised Cooling.

Resilience Level and Provisioning

- It is possible to build a single data centre to provide multiple levels of power and cooling resilience to different floor areas
- High resilience at the physical level is rarely an effective overall solution
- The minimum range for equipment to operate at, at the air intake to servers, is 18°C-27°C and 5.5°C dew point up to 15°C dew point & 60% RH
- From 2012, new IT equipment should be able to withstand the air inlet temperature and relative humidity ranges of 5°C to 40°C and 5% to 80% RH, non-condensing respectively, and under exceptional conditions up to +45°C

Temperature and Humidity Settings

- Data Centres should be designed and operated *at their highest efficiency* within the current environmental range of 18°C-27°C.

Free and Economised Cooling

Free or economised cooling designs use cool ambient conditions to meet part or all of the facilities cooling requirements, which can result in significant energy reduction (Table 7.1). Economised cooling can be retrofitted to some facilities. The opportunities for the utilisation of free cooling are increased in cooler climates and where increased temperature set points are used.

Table 7.1 Free-air cooling designs for data centres

Direct and indirect free air cooling systems	
Type	Description
Direct free air cooling	External air is used to cool the facility. Chiller systems are present to deal with humidity and high external temperatures if necessary. Exhaust air is re-circulated and mixed with intake air to avoid unnecessary humidification / dehumidification loads.
Indirect free air cooling	This involves using re-circulated air within the facility passed through a heat exchanger against the external air to remove heat to the atmosphere.
Limitations	Free and economised cooling technologies are more effective in areas of low ambient external temperature and or humidity. Most temperature climates including much of Northern, Western and Central Europe present significant opportunity for economised cooling.

7.2.2 Climate impacts on free-air cooling

The use of free-air cooling could be vulnerable to climate impacts. The use of fresh air from outside the data centre to support the cooling systems allows data centres to use outside air when the temperature is cool, but they often fall back on air conditioning on warmer days. As a result the data centre is much more reliant on the local weather and more accurate local forecasting. Improvements in free airflow around equipment and components, such as computer processors and chips, allow data centres to operate up to 26.7°C (80°F).

The use of free air-cooling has become common among larger companies. Intel have recently conducted a ten month trial in new Mexico to evaluate the use of only outside air to cool the plant, and has concluded that they found “no consistent increase” in the failure rates of machines using this method[11]. Other companies are also using these systems including HP, Yahoo and Microsoft.

Google have taken the use of free air systems a step further: their new plant in Belgium is reliant only on free air cooling and does not have any chiller systems.

[11] http://www.datacenterknowledge.com/archives/2008/10/14/google-raise-your-data-center-temperature/

7.2.3 Results from the UKCP09 weather generator for London data centres

Rather than using air-conditioning part-time in their free air-cooling system, Google has eliminated air-conditioning entirely. On the days when it is too hot to maintain cool temperatures, Google says it will turn off equipment as needed and shift computing load to other data centres. This approach is made possible by the scope of the company's global network of data centres, which provide the ability to shift an entire data centre's workload to other facilities. This system is currently in use at Google's data centre in Belgium. In this case study, we have used the UKCP09 weather generator to investigate the consequences of climate change on a similar system if it were operated in London (where Google also have a data centre). We considered the threshold temperature of 26.7°C in London, to identify how many days per year would be too hot for the free-air system to operate. We have also explored changes in humidity, since data centres must be maintained within an ideal relative humidity range of 40 to 55 % (although recently, best practice identifies absolute humidity rather than relative humidity as the key factor).

Baseline climate (1961-1990)

- The annual average number of **days above** the data centre threshold of **26.7°C** for passive cooling in London for the baseline is **5**, as a mean average number of events over the 1961-1990 **baseline** period. **All** of these **days occur** in **summer**.
- The annual average number of **days** where free cooling data centres **will not need to reduce their relatively humidity** (when relative humidity less than 55%) is **8** over the baseline period.

2030s (high emissions scenario)

- The annual number of **days above** the data centre threshold of **26.7°C** in London for the **2030s** is **21**, as a mean average number of events over the 30-year time period. **Two** of these **days occur either side of summer**.
- The annual average number of **days** where free cooling data centre's **will not need to reduce the relatively humidity** (when relative humidity less than 55%) is **8** over the 30 year time period of the 2030s.

2050s (high emissions scenario)

- The annual average number of **days above** the data centre threshold of **26.7°C** in London for the **2050s** is **34**, as a mean average number of events over the 30 year time period. **Four** of these **days occur either side of summer**.
- The annual average number of **days** where free cooling data centre's **will not need to reduce the relatively humidity** (when relative humidity less than 55%) is **11** over the 30 year time period of the 2050s.

2080s (high emissions scenario)

- The annual average number of **days above** the data centre threshold of **26.7°C** in London for the **2080s** is **58**, as a mean average number of events over the 30 year time period. **12** of these **days occur either side of summer**.
- The annual average number of **days** where free cooling data centre's **will not need to reduce the relatively humidity** (when relative humidity less than 55%) is **20** over the 30 year time period of the 2080s.

UKCP09 does not include any recognition of urban land-use and there is no incorporation of the Urban Heat Island effect.

7.2.4 Conclusions for data centre resilience

Data centres in London will need to be prepared for an increase in the number of days above the 26.7°C in the future. The number of days exceeding this threshold increases from 5 in the baseline, to 8 by the 2030s, 11 by the 2050s and increasing fourfold from the baseline by the 2080s to 20 days over the current operational threshold. Later in the century, some of the days when this temperature is exceeded also start to occur outside of the summer months. With regard to humidity, UK climate is commonly humid, with a need for dehumidification in order to maintain optimal conditions for data centre equipment. The results of this study show that with climate change the number of days when dehumidification will not be required (i.e. when relative humidity is below 55 %) may increase, from 8 in the baseline and 2030s, to 11 by the 2050s, reaching 20 days per year by the 2080s. For greater confidence in the humidity results, further work to explore changes in absolute humidity would be required (although these data are not available in UKCP09).

Our results confirm that the number of days per year on which external air is too warm to cool a data centre facility in London will increase significantly through this century. Many companies may end up using their chiller systems more often. One potential method for large companies to maintain low energy bills even on hot days is to switch the computational load to other data centres in their networks in cooler locations around the globe. However smaller companies are unlikely to have this multi-site advantage. The siting of data centres may become increasingly dependent on access to cool air for free air cooling systems; for example, HP have just opened a new data centre off the North Sea to access cooler air temperatures for this purpose[12].

Other actions taken by ICT companies in relation to increasing resilience against temperature increases could involve developing chips which will operate at higher optimal temperatures[13], reducing the need for cooling to the same extent. The deployment of data centres off-shore and in cooler climates (such as Siberia) is also expected[14]. However, these centres will also be at risk from climate change, in relation to rising sea levels, extreme weather, or melting permafrost. Climate change is likely to have an impact on all aspects of data centre location in addition to the difficulties it presents for free air-cooling. Google's main considerations when siting data centres currently include availability of green energy, proximity to rivers and lakes for water cooling, large areas of land, the distance to other Google data centres (for fast connections between data centres), and tax incentives. Several of these factors could themselves be vulnerable to climate change due to flooding, water availability, and land use changes as a result of novel flood management measures.

7.3 Case study: Climate impacts on rail and ICT

The impacts of climate change on ICT and other infrastructure sectors can be linked in complex ways, as shown the following two examples from East Coast Mainline.

7.3.1 Snow and ice affecting trains in January 2010

In the weather event of January 2010, there were multiple days with temperatures below 0°C and significant snowfall. Snow collected on the undersides of trains and the sustained weather conditions allowed this to build up and turn to ice. The result was that large blocks of ice (weighing up to 50 kg) were falling off the underside of the trains at high speed, bouncing up off the track and damaging components such as hoses and pipes. A number of trains were damaged, cancelled and / or stopped short of their final destination, for example, stopping at Edinburgh rather than continuing to Glasgow, Inverness or Aberdeen. The knock-on implications were blocked lines, mainly in Scotland. When the snow melted it resulted in floods that affected signalling and this caused further disruption.

The implications for ICT were:

- Customer Information Systems did not have up-to-date (real time) information some of which comes directly from track side detectors;
- The efficiency of WiFi on trains was affected by the weather conditions. People on the train use mobiles to update friends / colleagues more, which affects availability of bandwidth;
- There were increased enquiries from customers about the disruptions which resulted in congestion of the public information channels. e.g., National Rail Enquiries site, SMS text messaging on train arrival / departures, Train Operating Companies web sites etc;
- There were also occasional power issues that affected data rooms and servers.

[12] http://www.zdnet.co.uk/news/it-strategy/2010/02/12/hp-datacentre-taps-icy-north-sea-wind-40038511/
[13] http://www.theregister.co.uk/2008/10/15/google_and_intel/page2.html
[14] http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4753389.ece

7.3.2 Trains and ICT in high temperatures

Heat affects rail tracks because the rails can buckle. This is not a regular problem on older tracks which are short cut rail, and have expansion gaps left between the rail ends. However, for newer track, known as Continuous Welded Rail (CWR) the rails are pre-stressed and when laid are welded together making them vulnerable to expansion in high temperatures (above 26.5^{o}C). The benefit of CWR is that it allows trains to travel at 125mph compared to only 100mph on short cut rail. Speed restrictions are imposed on hot days often resulting in delays. Overhead power cables are also vulnerable to expansion during high temperatures and this has resulted in trains becoming stuck en-route with passengers on board. Carriages on high speed trains have no opening windows and rely on air conditioning systems within the compartments. This is particularly important for electric trains which unlike diesel trains have no on-board source of power. When overhead power cables are affected, lack of power means that a comfortable temperature (below 25 $^{\circ}$C) cannot be maintained within the carriages and passengers have smashed the windows to improve ventilation and reduce internal temperatures. Many trains carry additional water and food supplies for such emergencies.

The implications for ICT were:-

- It is currently not possible to reset the air conditioning modules remotely en-route and it can only be fixed once the train reaches its final destination;
- There were increased enquiries from customers about the delays resulting in congestion of the public information channels.
- In older data centres not designed specifically for the task, air conditioning is marginal in normal weather and it can often fail when temperatures go above 29 °C. The failure had impacts for operational systems, travel centres and ticketing systems.

8 Conclusions and Recommendations

8.1 Conclusions

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

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. By comparison with the other sectors, in ICT the physical assets themselves are not so significant.

Thus the climate issues are different and the sector is not as 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 therefore 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, whether that is 'ticketless travel' on public transport, electronic banking and other financial transactions, or electronic health records. National infrastructure, business and leisure activities are expected to depend increasingly upon uninterrupted availability of ICT services.

Weather presents disruption and challenge to the provision of services already, and increasing dependence on ICT means that the consequences of these 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 to increasingly frequent occurrences of weather disruption with new, more robust 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 the UK's dependence upon ICT will be affected by climate change occurring across the globe. 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 a smaller number of 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.

8.2 Recommendations

The study has identified 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 recommendations are summarised in Table 8.1, which also suggests which actors should be involved in each.

Table 8.1 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 *Infrastructure and Adaptation* 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		✓		✓

Summary of study recommendations identifying the relevant actors				
Recommendation	Government	ICT providers	ICT customers	Research community
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	✓		✓	

We offer the following recommendations for research and data development:

- A more detailed follow-up assessment of the direct climate change risks presented in Chapter 4, including an objective prioritisation and identification of the actors responsible for each risk. This would enable more concrete identification of the role that government will need to play in improving climate resilience in the ICT sector.
- A review of evidence of the impact of past weather events on infrastructure and ICT service providers. This would start to strengthen the business case for action on adaptation.
- Some specific research questions include examining how absolute humidity (dewpoint) may change under climate projections (as this is relevant to optimising the environmental conditions for IT devices), and examining potential changes in wireless signal based on temperature and rain rates in the UK Climate Projections.
- A policy study to review the potential role of government, the regulator, and existing market structures in addressing climate risks in the ICT sector. There is a wide range of policy options that could be considered to incentivize adaptation to address the climate risks identified in this study (including support for innovation in research, funding for demonstration projects, public sector co-investment in adaptation measures, measures to embed climate risk in the current market, regulatory incentives, etc).

We offer the following recommendations in relation to awareness-raising and engagement within the ICT sector:

- Follow up activities to raise awareness of the potential impacts of climate change on ICT, through the *Infrastructure and Adaptation* project, and linking with the Critical Infrastructure Resilience Programme. The study identified that there is still only a low base of awareness of climate change and its potential risks within the ICT sector. Awareness-raising and engagement sector-wide is highlighted as a priority.
- Workshops or collaborative efforts among the major telecommunications providers to build the business case for companies themselves to address climate risks. In particular, we note that while the major telecommunications providers are starting to address this issue, few have considered developing a climate risk management or adaptation strategy. Sector practitioners involved in our workshops and interviews were all positive about finding out more about the issue.
- Engagement within the sector to review models for ownership, roles and responsibilities in the context of climate resilience, from the perspective of the end user customers of ICT services.
- A horizon-scanning exercise to scope the long-term trends in the ICT sector more comprehensively and compare with climate change. (This could bring together futurologists, climate change experts, practitioners from military settings, etc.)

We offer the following recommendations in relation to engagement outside the ICT sector:

- Further cross-Government collaboration to explore interdependency issues,
- Better coordination of emergency response plans for weather events and ICT requirements/assumptions and better coordination of local authority resilience planning and ICT providers.
- Further investigation of supply chain security for ICT, particularly to comprehend the international dimension. Comparisons with work completed in the food sector might be relevant here.

We offer the following recommendations for climate risk management in the ICT sector:

- Government to consider how the IT industry may be drawn into the Critical Infrastructure Resilience Programme in future, alongside telecommunications infrastructure. Similarly, Government could review definitions of infrastructure across all of its National Infrastructure work in order to include IT aspects (not just telecommunications) within their scope.
- IT industry and telecommunications providers should commence corporate climate risk management programmes (in the context of their wider risk management strategies), building on existing climate awareness. These could take a dual approach: to identify long-lived assets and longer term strategies in the context of climate change and to focus on planning for extreme weather in other cases.
- IT and telecommunications providers to make greater use of weather-forecasting data for early-warning, and link into Environment Agency flood warnings where relevant to assets.
- Ongoing work to improve contingency and emergency recovery plans that respond to and reduce weather risk should be extended to cover a full range of weather events, and to consider how climate change may increase the frequency and severity of those risks.
- Customers of ICT services to become more aware and demanding of the climate resilience that they pay for. Procurement mechanisms could support this demand.

Glossary

Table of Acronyms

ACC	Adapting to Climate Change (Programme)
ATM	Automated teller machine
CCRA	Climate change risk assessment
CST	Council for Science and Technology
CWR	Continuous Welded Rail
Defra	Department of Environment, Farming and Rural Affairs
EDI	Electronic data interchange
EA	Environment Agency
GPS	Global Positioning System
ICT	Information and Communication Technologies
IEEE	Institute of Electrical and Electronics Engineers
IPCC	Intergovernmental Panel on Climate Change
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LCLIP	Local Climate Impact Profile
LA	Local Authority
NI	National Infrastructure
PDA	Personal Digital Assistant
RAF	Royal Air Force
SCADA	Supervisory Control and Data Acquisition
SMS	Short Message Service
UKCIP	UK Climate Impacts Programme
UKCP09	UK Climate Projections 2009
VOIP	Voice Over Internet Protocol
WEEE	Waste, Electronic and Electrical Equipment
WiFi	Wireless Fidelity

Terms and Definitions

Adaptation Adjustment in natural or human systems in response to actual or expected climatic stimuli or their effects, which moderates harm or exploits beneficial opportunities.

Climate Refers to the average weather experienced in a region over a long period, typically at least 30 years. This includes temperature, wind and rainfall patterns.

Climate change Refers to any change in climate over time, whether due to natural variability or as a result of human activity.

Climate impact A specific change in a system caused by its exposure to the climate. Impacts may be harmful (impact) or beneficial (opportunity).

Climate resilience *Resilience* to *climate impacts*. The ability of a system to absorb climate-related disturbances while retaining the same basic structure and ways of functioning.

Cloud computing Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and other devices on-demand, like a public utility.

Critical national infrastructure Those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life

Data centres Data centres house computer systems, server and network infrastructure and associated storage platforms. Many organisations operate their own data centres in house.

End-user devices These devices include computers –both portable and desktop, telephones, mobile telephones, PDA and other hand-held devices, SCADA control devices, GPS and transmitters/receivers.

ICT Information and Communication Technologies. The entirety of the networks, systems and artefacts which enable the transmission, receipt, capture, storage and manipulation of voice and data traffic on and across electronic devices.

IT Information Technology. Set of tools, processes, and methodologies (such as coding/programming, data communications, data conversion, storage and retrieval, systems analysis and design, systems control) and associated equipment (including computers and multimedia devices) employed to collect, process, and present information.

National Infrastructure Those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends.

Resilience An infrastructure element is resilient when, although dependent on other systems, it can continue to function effectively when one or more of those dependencies are broken. It can do this because there are multiple paths to enable its operation such that no single dependency failure can prevent its operation. “The ability of a system or organisation to withstand and recover from adversity”. A resilient organisation is one that is still able to achieve its core objectives in the face of adversity through a combination of measures (Cabinet Office, 2010)

Risk Hazards or events that could have an impact on exposure to danger or loss. Climate risks are additional risk to investments (such as buildings and infrastructure) and actions from potential *climate impacts*.

Telecommunications 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.

UKCP09 weather generator and threshold detector A downscaling tool that can be used to generate statistically plausible daily and hourly time series comprised of set of climate variables at a 5 km resolution that are consistent with the underlying 25 km resolution climate projections.

Virtualisation Virtualisation means running software within a virtual environment. Virtual environments are created when operating systems and desktop applications are emulated, and don’t run directly on physical hardware. When software is virtualised, you can run several applications and operating systems on one physical server.

Vulnerability The degree to which systems are susceptible to, and unable to cope with, adverse impacts.

Weather Refers to the state of the atmosphere as experienced now, with regard to temperature, cloudiness, rainfall, wind, and other meteorological conditions.

References

The following sources were consulted during the course of this study.

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

AEA (2009b) Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector. Report to the European Commission.

AEA (2009c) Scoping Study for a National Climate Change Risk Assessment and Cost-Benefit Analysis. Report to Defra.

BBC News (2009) Cumbria floods: Body found in hunt for policeman. http://news.bbc.co.uk/1/hi/uk/8369934.stm [accessed 16/03/2010]

Betts, R., Sanderson, M., Hemming, D., New, M., Lowe, J. and Jones, C. (2009) Presentation at 4 degrees and beyond conference, Oxford. http://www.eci.ox.ac.uk/4degrees/ppt/1-2betts.pdf.

California Natural Resources Agency (2009) California Climate Adaptation Strategy http://www.climatechange.ca.gov/adaptation/

Cabinet Office (2008) National Risk Register http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx

Cabinet Office (2009) Security for the Next Generation – The National Security Strategy of the United Kingdom: Update 2009 http://www.cabinetoffice.gov.uk/reports/national_security.aspx

Cabinet Office (2010a) Strategic Framework and Policy Statement. Available from www.cabinetoffice.gov.uk/ukresilience/infrastructureresilience.apsx

Cabinet Office (2010b) Sector resilience plan for critical infrastructure. Available from www.cabinetoffice.gov.uk/ukresilience/infrastructureresilience.apsx

Cabinet Office (2010c) Interim guidance to the economic regulated sectors. Available from www.cabinetoffice.gov.uk/ukresilience/infrastructureresilience.apsx

CEH (2009) UK Flooding – Briefing from the Centre for Ecology & Hydrology - 20 November 2009, Jamie Hannaford, Centre for Ecology & Hydrology http://www.ceh.ac.uk/news/news_archive/2009_news_item_48.html [accessed 16/03/2010]

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

Data Centre Knowledge (2008) Google: Raise Your Data Center Temperature, October 14th, 2008. http://www.datacenterknowledge.com/archives/2008/10/14/google-raise-your-data-center-temperature/

Defra (2009) Engineering, Infrastructure and Climate Change Adaptation Conference, ‘Engineering to ensure long-term climate resilient infrastructure’, Report of Proceedings.

Defra (2010a) The role of government in adaptation. http://www.defra.gov.uk/environment/climate/adaptation/government-role.htm

Defra (2010b) Adapting your procurement: Summary, Report with Office of Government Commerce (OGC), Crown Copyright http://www.defra.gov.uk/environment/climate/documents/procurement-sumary.pdf

DCMS and BIS (2009) Digital Britain http://www.culture.gov.uk/images/publications/digitalbritain-finalreport-jun09.pdf

Garnaut Climate Change Review (2008) Impact of climate change on Australia's telecommunications infrastructure.

Greater London Authority (2010) The draft climate change adaptation strategy for London Public Consultation Draft
http://www.london.gov.uk/climatechange/sites/climatechange/staticdocs/Climiate_change_adaptation.pdf

House of Commons (2010) Adapting to Climate Change, Environmental Audit Committee, Sixth Report of Session 2009–10
http://www.publications.parliament.uk/pa/cm200910/cmselect/cmenvaud/113/113.pdf

IEEE Computer Society (2002) IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture http://standards.ieee.org/getieee802/802.16.html

Institute of Mechanical Engineers (2009) Climate Change, Adapting to the Inevitable?
http://www.imeche.org/NR/rdonlyres/D72D38FF-FECF-480F-BBDB-6720130C1AAF/0/Adaptation_Report.PDF

Institution of Civil Engineers and Building Futures (2010) Facing up to Rising Sea-Levels: Retreat? Defend? Attack? The Future of our Coastal and estuarine cities
http://www.ice.org.uk/downloads/Facing%20Up%20to%20Rising%20Sea%20Levels%20Document%20Final.pdf

Intellect (2010) General Industry Fast Facts http://www.intellectuk.org/content/view/4348/377/#general

Intellect (2008) High Tech: Low Carbon The role of technology in tackling climate change
http://www.intellectuk.org/content/view/775/84/

Intellect (2007) Software and IT Services Report – The Future
http://www.intellectuk.org/content/view/775/84/

IPCC (2007) Fourth Assessment Report http://www.ipcc.ch/

JRC (2010) 2010 Best Practices for the EU Code of Conduct on Data Centres, Version 2.0.0 Release
http://re.jrc.ec.europa.eu/energyefficiency/pdf/CoC%20DC%20new%20rep%20form%20and%20guidelines/Best%20Practices%20v2.0.0%20-%20Release.pdf

Jenkins, G.J., Perry, M.C., and Prior, M.J. (2009) The climate of the United Kingdom and recent trends. Revised edition, January 2009. Met Office Hadley Centre, Exeter, UK.

London Climate Change Partnership (2010) London Adaptation Strategy
http://www.london.gov.uk/climatechange/

Mann, B. (2009) Head of the Civil Contingencies Secretariat. What are our key responsibilities?
http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx

Murphy, J.M., Sexton, D.M.H., Jenkins, G.J., Boorman, P.M., Booth, B.B.B., Brown, C.C., Clark, R.T., Collins, M., Harris, G.R., Kendon, E.J., Betts, R.A., Brown, S.J., Howard, T. P., Humphrey, K. A., McCarthy, M. P., McDonald, R. E., Stephens, A., Wallace, C., Warren, R., Wilby, R., Wood, R. A. (2009), UK Climate Projections Science Report: Climate change projections. Met Office Hadley Centre, Exeter.

RCEP (2010) Adapting Institutions to Climate Change: Summary Report, Royal Commission on Environmental Pollution http://www.rcep.org.uk/reports/28-adaptation/28-adaptation.htm

Shukla, Dr A. (2006) UK climate change - Impact on radio systems QinetiQ Proprietary

The Register (2008). Google demanding Intel's hottest chips? Inside Project Will Power http://www.theregister.co.uk/2008/10/15/google_and_intel/page2.html

The Times (2008) Google search finds seafaring solution. September 15, 2008 http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4753389.ece

URS (2010) Adapting Energy, Transport and Water Infrastructure to the Long-term Impacts of Climate Change

Victoria Government (2006) Climate Change and Infrastructure, Planning Ahead

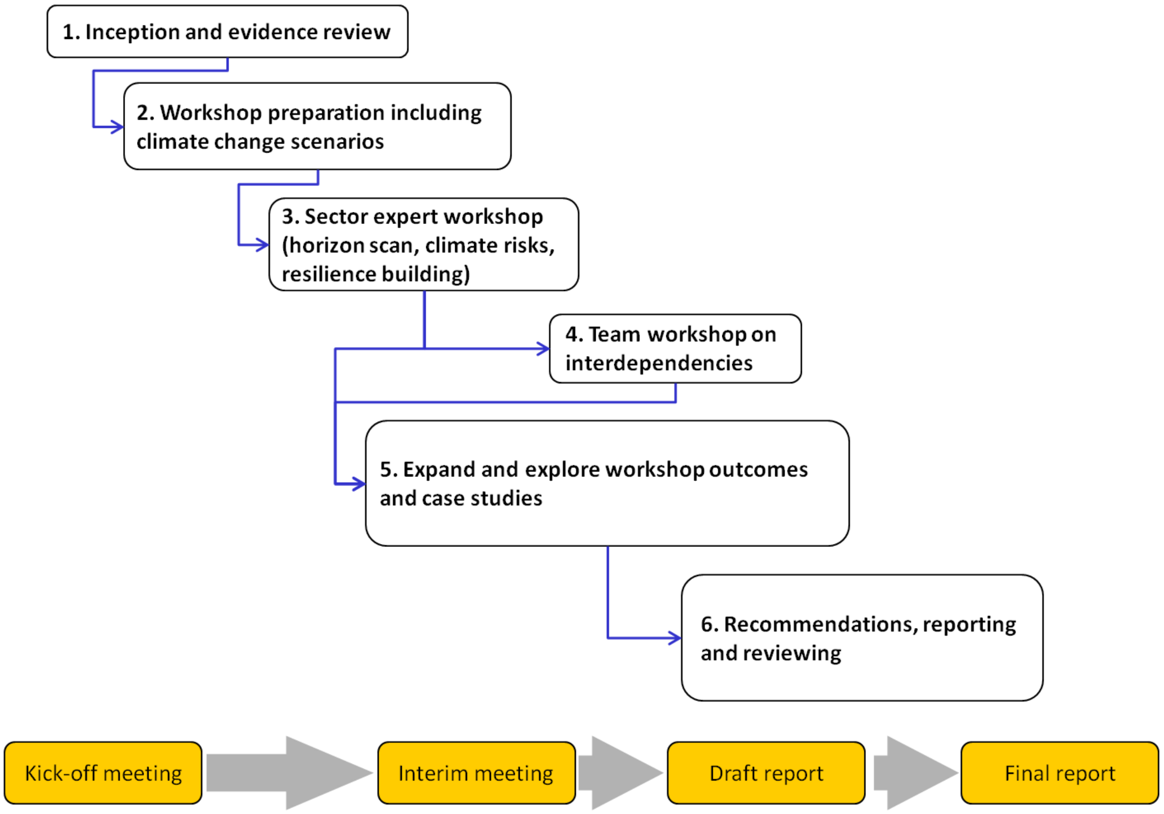
Williams, N. (2009) The In House Policy Consultancy, Infrastructure and Climate Change Adaptation Project, Workstream 1 Part 1, Final Report, Serving CLG, DfT and Defra

Zdnet (2010) HP datacentre taps icy North Sea wind http://www.zdnet.co.uk/news/it-strategy/2010/02/12/hp-datacentre-taps-icy-north-sea-wind-40038511/

Appendices

Appendix 1 – Project Methodology

AEA used a six stage approach to achieving the aims of the work. The Tasks are shown in the diagram below.


1. Inception and evidence review
2. Workshop preparation including climate change scenarios
3. Sector expert workshop (horizon scan, climate risks, resilience building)
4. Team workshop on interdependencies
5. Expand and explore workshop outcomes and case studies
6. Recommendations, reporting and reviewing
Kick-off meeting
Interim meeting
Draft report
Final report

Task 1: Inception and evidence review

The Inception stage began with a kick-off meeting with Defra, which was essential to ensure that this project delivered to its aims and meets Defra's expectations within the timeframes available.

The purpose of the Evidence Review was to ensure that the project builds on and does not duplicate previous work on impacts and adaptation for infrastructure in the telecommunications/ICT sectors. We reviewed and synthesise existing knowledge on the long-term impacts of climate change on the sector.
This was not an exhaustive literature review, but served to identify what is currently known, and to avoid duplication in the rest of the project. Documents were carefully chosen so as to ensure that a clear and robust synthesis of current knowledge was produced.

Task 2: Workshop preparation

In advance of the workshop we carried out targeted preparation activities to provide the basis on which to focus the discussion. This was needed to ensure best use of the limited time of the expert panel. The main areas of preparation were:

- Categorisation of the sector and its characteristics
- Identification and invitation of experts representing all aspects of the ICT sector to participate in the workshop (ideally to include coverage of academia, policy/government, regulators / standards, technical/networks, services / distribution, and practitioners in related sectors like rail)

- Development of appropriate climate scenarios to form basis of discussion (based on UKCP09) We also developed an overview of climate change at the global level.
- Design of workshop, briefing and materials for the sessions.

Task 3: Sector expert workshop

The sector expert workshop was a central task in this project. Because there is relatively little published literature examining the impacts of climate change for ICT / telecommunications, the workshop provided the quickest way to engage real experts working in the sector to identify potential risks and possible solutions in the context of the long term future for the sector.
The workshop was structured around key questions:

- What are the future developments in ICT over the next 20 and 50 years, or longer term?
- What are the implications for technical standards?
- What challenges/opportunities do these present? For operations, standards, supply chain (esp. ownership), reputation?
- What risks (in general) will become present and/or increase? What risks related to weather/climate will emerge or reduce?
- How is resilience currently built into ICT infrastructure (and plans for the future)?
- How can resilience, especially climate resilience, be increased and barriers be overcome?
- What are the business/economic challenges, and opportunities, that this will generate?
- How does the regulatory regime enable/inhibit resilience?

Task 4: Team workshop on interdependencies

The specification had a particular concern to explore interdependencies of telecommunications /ICT with other infrastructure sectors in the context of long-term climate change. In order to give adequate attention to this aspect, we held an internal project team workshop to identify critical interconnections and interdependencies in this regard. The workshop was planned in detail during the project, and among others considered the following questions:

- How can the impacts on the telecommunications/ICT sector affect others – how far is the sector an essential element for the operation of other sectors?
- What awareness is there within the telecommunications/ICT sector to these interdependency impacts?
- How climate change impacts on other sectors affect the telecommunications/ICT sector? What awareness is there of these risks?
- To what extent will a cross-sectoral approach to building climate resilience be important for national infrastructure?

Task 5: Expand and explore workshop outcomes and case studies

We explored in detail the outcomes from the workshop. We followed-up specific ideas with individuals to develop domestic and international case studies of impacts and potential adaptation in the sector. This Task looked to build additional evidence to support the outcomes and ideas voiced at the workshop.
As part of this task, identified a portfolio of possible adaptation measures that could enable the telecommunications / ICT sector to be adapted for climate change over the next 30 years or so (since this is now set by past levels of greenhouse gas emissions), and then adaptable to cope with a range of possible climate futures thereafter.
In relation to barriers, we looked to expand upon the views emerging from the workshops.

Task 6: Reporting

All of the analysis from the project was drawn together into this final report. Recognising that the project report should also be accessible in the sector / to industry, we have maintained links with some of our expert panel to ensure that it is targeted appropriately. We have been particularly concerned to provide a clear structure, good use of real-life examples and case study material, visual or diagrammatic presentation where possible and appropriate, and an overarching emphasis on the critical role of ICT.

Appendix 2 – Sector Expert Workshop Report

ICT climate change resilience expert panel: Workshop report

Wednesday 3rd March 2010. IET, Savoy Place, London.

Summary

Climate-related risks identified during the workshop that were considered the most important (red dots):

- Flood impact on terrain/ other assets e.g. bridge
- Power/resilience
- Flooding – immersion – more seasonal and increased intensity
- Rain – anything subsurface: siting of data centres – drivers of community and environment
- Temperature – modelling of wireless coverage is temperature dependent (depends on refractive index) – decisions on location and density of masts
- Drought and subsidence – structures unstable
- Secondary impacts e.g. flood damage to roads exposing cables and bridges – e.g. Cockermouth
- Changing vegetation type (or land-use) – impact on RF propagation (depends on seasonality)
- Decrease in serviceable lifespan of structures
- Greater certainty in likelihood and impact
- Climate change could lead to bidding wars over precious commodities in future e.g. gas/metals. Resource scarcity – protectionism e.g. wood?

Key issues on improving the resilience of the ICT sector that should be considered within the project:

The attendees were requested to list the 3 issues they considered the more important within the sector (from the feedback forms)[15].

Technology

- The technology will move towards virtualisation and from micro to nano technology.
- What is the impact on the resilience of the ICT sector of outsourcing and cloud computing on a global scale?
- Understand what materials are used/will be used in the future, in data centres/ PCs, where are they sourced from, what are the risks?
- Being able to differentiate systems or devices offering greater resilience from those that did not
- There is the potential for the sector to be a leader in low-carbon technologies (mitigation) i.e. reducing energy demand/renewable energy use. How can we get hold of mitigation and climate risk and resilience together?
- Diversity can offer greater resilience. Diversity can mean different things – multiple layers of same infrastructure, or interoperability across different types of network
- Consider other technologies that can enhance resilience by supporting adaptability and flexibility of operation: “chameleon” technologies, reprogrammable, etc
- Explore resilience to climate impacts in the context of the whole network, rather than focusing in on individual resilience of particular nodes or sites.

[15] This is a SUPPLY–side view as there were no representatives at the workshop from the DEMAND-side to represent the end-user. It would be useful to receive any views that may demonstrate the opinions of end-users

- Can build on a good record of continuity and resilience in the sector: use the mechanisms in place, standards, etc. Avoid recourse to greater regulation in order to address this issue.

Planning, Regulation and Market/economic Forces

- The benefits a network set up can bring in terms of resilience (to all things) through diversity
- To date the market has made itself resilient through competition and good practice – NOT regulation- a lot can be achieved through the former
- We need more work on futures and what the system will look like. Need to bring together futurologists, climate experts to investigate further
- Flooding is probably the greatest risk to both ICT and key business sectors in the UK
- Planning needs to be long-term and cover different scenarios
- Develop early warning systems to link weather/climate forecasting with telecommunications providers to improve response to extreme weather events. Better information is required to understand where resilience could be achieved, could be helped by collecting evidence of impacts in the sector attributable to climate change
- What is the business case/demand for change? Addressing behavioural barriers to building climate resilience – how to create market pull or policy push to encourage more resilient products / services

- We cannot drive this (sector) it needs to be driven by Government/customers/market
- Changing infrastructure to more resilient forms / new standards – in general can happen as part of regular refresh programmes eg mobile handsets. But some situations in which you cannot just refresh parts of the infrastructure – e.g. Air Traffic Control, nuclear industry – have longer investment and planning timeframes (25 years) - so should be planning now for next systems.
- Growth of ICT and reliance upon it will continue to increase rapidly in future, therefore important to address issue of climate resilience as otherwise potential risks / disruption across many sectors is likely to magnify
- How do we create economic pull-through for greater resilience without moving to a completely new regulatory framework?

Interdependency

- The interdependent nature of different infrastructures
- UK is not an island, there is global interconnectedness and dependency
- ICT is pervasive and impacts the whole of the UK economy
- There are climate impacts on ICT systems
- There is a need for greater resilience in ICT, less dependency on an individual suppliers/countries
-

Costs

- Continuing the practice of new build on flood plain builds in inherent cost
- Resilience costs - someone needs to pay

Information needs and knowledge sharing

- There is a need for better information (more granularity) to aid business planning
- Data is critical to understanding the effects
- We need to learn from each other – collaboration on this issue will help
- We are good at resilience, continuity and recovery, we should build on that and add climate into this process

- Transferring knowledge from those already doing resilience work e.g. from other countries or sectors (defence). Other technologies use assets more effectively - ICT solutions could be chameleon and fibre optic cable.
- Learn from disaster planning continuity that the UK does well – sources?
- Where can the sector find data to help with decision making?
- Awareness raising /education about the issue across the sector

Social

- Social impact and view that will make changes in demand - Need to look at social drivers e.g. a train fails to run, people sort themselves out only a few create confrontation.

---

1. How does the weather affect telecommunications?

- Overheating in data rooms etc
- Spacewire – chameleon like approach to technology, reprogrammable devices
- Lightning strikes on transmitters
- Wind loading on masts
- Flooding of conduits e.g. fibre cables etc
- Sunspot activity affects satellite communications
- Mobile recovery networks for disaster relief via RF!
- Rainfall rates severely impact quality of service
- Wet weather call volumes
- RF – precipitation learn from industrial deployments – JSA 100 – Reference existing bodies
- Average max temperature, what about peak changes in continuous high temperatures?
- Increased snowfall impacts antenna
- Adverse weather increases scale of faults makes it harder to repair/ restore
- Very cold weather reduced efficiency of underground cables?
- Impact on network resilience
- Increased occurrence of fog for free space optics links
- Temperature changes impact coverage of wireless signals

Exercise 1: What are the current vulnerabilities and critical thresholds for infrastructure / standards? How do these compare with key climate variables?

The overall issue is that for any weather event there is disruption of services and that the repair and maintenance needs staff and equipment (resources). This resource is unreliable (e.g. sickness, excuses to go sledging! Holiday) so planning for such events so that resources are available is a key element of maintaining services.

- Rain/flood
  - issue is to seal the network from water ingress,
  - density of rain drops affects signal,
  - snow and ice thaw causes a water surge
  - Flood – main issue was cabinets – now its bridges – snow melt
  - Communications systems along transport routes are vulnerable to flood
  - SME’s basement – lack of planning
- Snow
  - loading weight on cables,
  - problems of resource access, health and safety of staff – more slips/trips/falls, antenna tilt affects signal

- Ground
    - bridges e.g. bridge collapse in Cockermouth isolated an exchange,
    - 1987 storms caused subsidence and duct failure.
- Temperature
    - humidity – mobile networks,
    - Buildings - tolerance variability, H&S issues for staff.
    - Data centre cooling if temperature increases – no additional power available to cool, costs increase by 4% for each 1^{o}C of cooling.
- Wind – overhead cables at risk, need resources to repair
- Lifetime of the kit– it will have to tolerate change in temperatures/ humidity that it was not designed for. Often elements of the network are old and fine e.g. cables but some need regular updating e.g. connections
- International – India floods service levels in UK
- Built environment
    - Many buildings were never originally designed as data centres
    - Lack of sustainable urban drainage systems (SUDS),
    - Universal service obligation and fluvial planning means that BT still have to provide services to vulnerable sites i.e. in flood plains
    - Network infrastructure – ICT used to be just a phone service now it's a lifestyle choice e.g. building management and billing from smart metering, entertainment system, working from home. The impact if it goes down is much more severe so infrastructure needs to change to maintain service delivery.
- Voice communications – multiple networks – therefore alternatives/ contingency if single sites fail
- Grid at capacity in places
    - There are places where new data centres are not allowed (e.g. Canary Wharf)
    - Dependence of ICT on energy is limiting vulnerability

Exercise 2: How will the sector develop over climate change timeframes? What are the emerging technologies and connectivity issues?

2. Up to 2030's

- Globalisation: economic incentive to build kit to use globally – more likely now sector based on IP based networks
- Multifunctionality
- Less reliance on grid power for end users
- Cheaper communications = more communications
- Greater mobility
- Smaller and more efficient
- Fibre-based network (not copper) – inherently more reliable
- Hand held devices
- Reprogrammable kit e.g NASA satellite life has been radically extended
- Wireless connectivity
- Real-time data reliance
- New and modern – mixed population 50% can use 'thumbs' i.e. are ICT literate, 50% cannot.
- Data storage off site
- Changes would be driven by economics and resource
- Voice recognition - Biometrics
- Increase in data rates –
    - mobility of staff – converged – mix of technology working

  - RF Spectrum – broad range higher frequency bound (miniwave)
  - Copper to fibre

- Developing countries make technology leaps
- Community relies more and more on connectivity for diverse reasons!
- Clever technology e.g. health - remote operations in multiple places/ real time collaboration and 24 hour continuity coverage across time zones
- cloud and smart communities, end-user functions increase
- interactive – 2 way communications

2050's

- 24 hour communications globally
- Centralised control and management
- Bigger data centres, specialist ICT providers – located anywhere in the world
- Concentrated into super-monolithic networks – continuing existing trends (but greater resilience)
- Interaction of infrastructure and planning systems
- satellite networks – reliance on GPS
- All use thumbs – technology aware population will drive a change in infrastructures
- Progress increases
- More resilience in RF needed as all mobile
- Access hopper network – delivery network change mesh/ connectivity
- Dynamic and reconfigurable technology at the user end
- Intelligence/analysis – mammogram analytics – energy usage data mass analysis

3. Beyond

- Very little physical infrastructure
- No satellite communications
- No 'broadcasting', more peer to peer
- All indoors – change in social lifestyles
- Major increase in dependency on ICT for life - both lifestyle and fundamentals of life

---

<u>Exercise 3: What are the potential climate change threats (and opportunities) in the sector?</u>

Opportunity

- More energy efficient and renewable energy sources changes the infrastructure focus e.g. Use data centre as a heat source for the building, will reduce cooling needs for data centre and reduce heating needs in the building
- use technology to force a change in behaviour and pricing e.g. reduction in energy use – flex computing/ virtualisation around the globe
- Early warning offset system to decrease costs of mitigation 99.99 to 99.9.
- more sensors to give better planning e.g. tsunami advance warning system

Risk

- There is a risk that without the right climate information for business to make sound judgments, resilience planning will not take place. Companies will wait for the 'stick' e.g. tax or legislation instead of taking the 'carrot' understanding of climate. Need detail and certainty
- Concern over 'who owns the problem'
- Business needs a translation of climate science data into facts they can use – importance of messaging
- Risk as the dependency on ICT increases

- loss of ICT can be critical e.g. hospital
- Impact on data flows - pinch point
- Globalistation and supply chain risks
- More risk of global issues/events
- Greater mobility and home working
- Individual risks or connectivity may increase
- Overall for a company risk of weather events taking network out decrease
- Climate resilience becomes a commodity you pay for
    - more consumer choice? – but what about data protection

4. Exercise 4: What are the physical risks from climate change on the ICT sector?

UK risks

- Decrease in serviceable lifespan of structures
- Technology: refresh rates increase life of kit reduces
- Quality of service/ availability
- AC less to plant – resource management
- Power/resilience
- Remote locations

- Humidity
    - corrosion –
    - masts –
    - connectors for cables
- Flooding
    - Immersion
    - impact on terrain/ other assets e.g. bridge
- Rain
    - anything subsurface: siting of data centres –
    - drivers of community and environment,
    - more seasonal and intensity,
    - Intensity of rainfall – wireless impact,
    - work interruption (Ingress),
- Haze/visibility decreases – affects laser and free space communications
- Sea Level Rise
    - coastal erosion – coastal location –exchanges
    - water table/ saline intrusion
    - changing reference data for recalibration e.g. remote monitoring modelling of coastline
- Temperature
    - modelling of wireless coverage is temperature dependent (depends on refractive index)
    - decisions on location and density of masts
- Drought and subsidence
    - structures unstable – especially older structures as clay soils dry out or rehydrate,
    - Equipment overheating/cooling
- Snow
    - freeze thaw
    - snow/ice loading on cables, antennas, masts, poles
    - managing thaw,
- Ground temperature
    - copper wire performance improves at colder temperatures
    - variations

  - could cause connectors to fail

- Secondary impacts e.g. flood damage to roads exposing cables and bridges – e.g. Cockermouth
- Changing vegetation type (or land-use) – impact on RF propagation (depends on seasonality)

5. Global risks

- Some products/materials have unique provenance or unique processes
  - e.g. materials for masts, telegraph poles – climate impacts in sub-arctic
- Call centres in sub-continent and data centres – local weather impacts on employees and sites
- s/c sourcing/location of s/c – risk – cost – Netherlands – India
- Vulnerable to shipping disruptions from weather
- Transport disruption from severe weather – impact on ICT demand
- Evaluate off-shore location risk
- Climate change could lead to bidding wars over precious commodities in future, i.e. gas/metals. Resource scarcity – protectionism e.g. wood?
- Radio spectrum as a commodity at international level – competition for those parts of the spectrum which have greatest environmental resilience

---

Exercise 4: What are the knock-on implications of climate risks in this sector for other infrastructure sectors (energy, transport, water), and for business generally?
Exercise 5: What can be done to increase resilience to climate risks (in the context of the wider interdependencies)?

- Cross-sectoral vulnerabilities – transport, power, telecoms can suffer from same regional/local severe weather, But ICT can help by reducing critical dependence on transport
- Business – logistics highly dependent on ICT – e.g. agriculture
- Transport – smart containers – monitor T of contents – sensory IT devices more important
- Farmers (some) now use GPS as basis of planting, cropping and yield management
- Environmental monitoring depends on ICT
- Communications and energy dependency is the overarching priority
- Continuity of service verses mechanism/infrastructure
  - Wireless
  - Voice
  - Fixed
  - Data
- Data and information is key for panning in all sectors
- Abstract climate risk from standard business continuity risk – Hard
- Community response positive or negative
- Power stations – operating performance procedures require three separate routes to be maintained in order to keep nuclear power station running – when the Cockermouth bridge collapsed, 1 route was lost, and one other bridge was on the list of 12 ‘at risk’ bridges, if that bridge had failed, the power station would need to be shut down.
- Many control systems for other industries use ICT and are critical to the performance/maintenance of their services e.g. water resources (pumping) and sewage treatment
- Boats – Could provide access to plant during flood. Could also use remote communications but what is the risk of these failing?
- Many valves are controlled remotely by ICT e.g. Adelaide a boy hacked into the ICT system and caused the valves to open and flood the main street with sewage.

- The greater the frequency of an event the more likely it is that a procedure, tools and capability will be put in place to deal with this type of event.
- Remote ICT controls a huge variety of critical systems
    - air traffic control (ATC)(also wind farms create turbulence/scintillation? that can affect the signal for ATC)
    - banking (ATMs/credit cards)
    - Traffic lights e.g. thrustborer broke cable in tunnel and took out London's traffic lights.
- Government and local services e.g. LA snow plans (Cumbria and Northumberland A66), those LAs with good plans could clear roads effectively and allow BT to maintain a service more easily. Both - staff getting to work and staff and equipment getting to site
- Currently for defense all networks are connected so if one goes down there is an alternative – high resilience. Only works for 999 calls in UK. But if mobile operators share masts and network density reduces/ or a satellite is taken out ie the physical network is damaged –low resilience.
- Currently there are multiple routes available so that comms can be maintained in an emergency (landline/voice/text/change network)– high resilience. But how will this change in the future and will this increase or decrease resilience?
- The closer the failure is to the premises has an impact on the scale and extent of the outage.

    Need to find out how resilient the network is today and for what purpose ie emergency vs social chat/work. BTs 999 outage report could provide data on the timescale and extent of outages and allow us to calculate the cost of making the service more resilient and consider adaptation options.

Exercise 6: What are the barriers to building resilience? Are there some enablers?

Business level

- Create economic pull through market mechanisms to enhance resilience
- Greater certainty in likelihood and impact
- How do you get people to pay more for greater resilience? Customer demand/willingness to pay/brand impact
- Have better contingency plans for range of hazards
- Diversity of systems/ interoperability = ensure a level of redundancy and add in strategic/ dynamic nodes – specific locations where interconnectivity is allowed under disaster
- Early warning e.g. flood warning and weather data – telecoms operator
- Specific location/environmentally appropriate design e.g. for data centres and interdependent design authorities
- Learn from systems in other countries – e.g. Norway e.g. countries dealing with natural hazards – Iceland? e.g. compare/contrast tolerance of critical components
- Faster refresh rates with eco-design and software designed architecture and shorter lifetime components
- Modular approach
- How do you differentiate between systems offering more/less resilience? – Evaluation criteria? Standards? – need better understanding of risks to identify these
- Investment cycles, strategic planning timeframes and political timeframes on election cycle are all too short! Need for regulation
- Enabler –Oil companies (BP/Shell) share data to gain sector information although they are strong competitors too! The sector should do the same. May need pushing from government and regulation to achieve it. Need to determine sharing protocols eg security and privacy issues.
- Design for a different range of future climate. Can normally squeeze more out if than expected both lifetime and operational ranges. Very expensive to design for all factors, some areas will be commoditised and some will be bespoke. Design for a wider range of futures is difficult –

how do we do it? – More detailed data? – working with uncertainty- evidence of impacts to make the business case for new/ different design.

- How do you design a resilient data centre when it includes a range of ages for kit?
- Insurance premiums may drive behavior into considering long-term horizons for planning.

Society level

- Work out where you want to live and how do you need to spend your money
- communication rules
- Deal with behavioural barriers

Agenda

10:00	Coffee and comment board
10:20	Welcome • Brief welcome from Nick Coleman on behalf of the IET IT sector panel • Introductions around the table
10:30	Introductory presentations • Project context • Climate change scenarios
11:00	Exercise 1: What are the current vulnerabilities and critical thresholds for infrastructure / standards? How do these compare with key climate variables?
11:30	Exercise 2: How will the sector develop over climate change timeframes? What are the emerging technologies and connectivity issues?
12:00	Exercise 3: What are the potential climate change threats (and opportunities) in the sector?
12:30	Lunch, via "exit poll"
1:30	Exercise 4: What are the knock-on implications of climate risks in this sector for other infrastructure sectors (energy, transport, water), and for business generally?
2:00	Exercise 5: What can be done to increase resilience to climate risks (in the context of the wider interdependencies)?
2:30	Exercise 6: What are the barriers to building resilience? Are there some enablers?
3:00	Wrap up discussion • Key issues for the project to explore further • Recommendations
4:00	End

Attendees

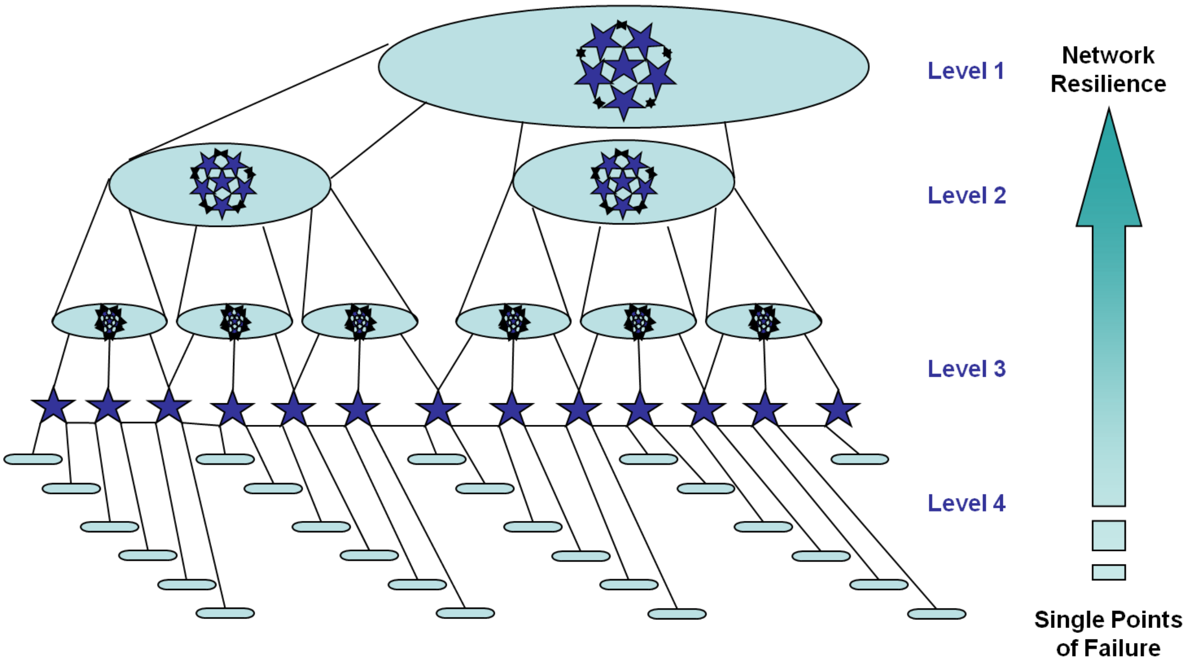
Name	Organisation
James Robbins	Abellio
Clare Downing	AEA
Lisa Horrocks	AEA
John Beckford	Beckford Consulting
Alice Reeves	BIS
Neil Barnes	BT
Ian Hill	BT
Will Lochhead	Defra
Tom Ramsay	East Coast Mainline Co
Andy de Clerck	Geode Networks Europe
Nick Coleman	IBM
Emma Fryer	Intellect
Ben Willis	OfCom
Anil Shukla	Qinetic

Feedback on the workshop

1. Very useful – new perspectives for me
2. Very good, would like to continue to be involved
3. Very enjoyable
4. Good fun, nice network. Perhaps a wider field is required:
   a. 1) other countries, 2) futurologists, 3) EDF/nuclear power etc.
5. Interesting day

Appendix 3 – A model for resilience in ICT

The study found that there were different opinions about what constituted the resilience of the ICT network. We established the model illustrated in the diagram below to show that perceptions of resilience at different levels and from different perspectives are equally valid.



The diagram shows how:

At level 4 – an individual user will have access to the ICT networks via a singly connected device (i.e. the user has only one connection to the system via that device). However, at the same level, each user may have more than one device (a landline, a mobile phone, VOIP access). Each device represents a user level single point of failure.

At level 3 there is increased resilience with each individual access point providing multiple possible pathways from one user to any other user – at this level the single point of failure may be a local exchange, switch box or point of presence – i.e. it is a system failure local to the user.

At level 2, the resilience is again higher with large elements of the whole system able to function and, almost, no single point of failure – but when there is a failure the number of people affected is significant (for example, flooding at a BT exchange in London, as occurred in March 2010).

At level 1, the resilience of the whole system is such that complete failure is highly unlikely; there are minimal potential single points of failure at that level as dynamic rerouting at lower levels will bypass any specific problem areas.

As can be seen, resilience increases as we move through network levels from the individual user up to the system as a whole.

Appendix 4 – Review of CDP 2009 responses

Companies provide responses to the Carbon Disclosure Project based on their environmental concerns and performance. Within the 2009 survey they are asked to respond to three questions relating to how they view the risks from climate change. These questions are:

1. Is your company exposed to regulatory risks related to climate change?
2. Is your company exposed to physical risks from climate change?
3. Is your company exposed to other risks as a result of climate change?

This study has analysed the responses to the second and third of these questions by four companies within the ICT sector, to provide an indication of how climate change risks are viewed within the sector. These companies were chosen as a best fit across the telecommunications sector as leading phone, television and internet providers.

In answer to the second question, companies identified a large number of direct physical risks from climate change, and these varied from one company to the next. The key physical risks they identified are shown in the table below.

Company	**Storm or flood-related risks**	**High temperature related risks**	**Sea level rise or coastal erosion risks**	**General business disruption from weather events**	**Property or equipment damage**	**Customer complaints from service failures**
BSKYB				✓	✓	
Cable & Wireless	✓	✓	✓			
Vodafone	✓	✓			✓	
BT Group	✓		✓	✓	✓	✓

Companies also identified additional knock-on risks from climate change, as shown below.

	Knock-on risks from the physical impacts of climate change
BSKYB	1. Risk to pension assets linked to companies or regions affected by climate change. 2. Changes in insurance availability and increases in premiums due to higher exposures to climate-induced risks.
Cable & Wireless	None identified
Vodafone	Increased demand due to humanitarian disasters Supply chain risks Material and mineral price increases Longer term possible risks include political responsibility and restrictions on travel
BT Group	Customer perception

The diversity of risks and impacts identified across the four companies may reflect their different experiences of the consequences of weather events to date. As these companies make progress in their own work to assess and manage climate risks, a growing consensus may emerge around the particular issues that will present greatest concern to providers in the ICT sector.

AEA group
329 Harwell
Didcot
Oxfordshire
OX11 0QJ

Tel: 0870 190 3862
Fax: 0870 190 6318