Adapting to Climate Change
Environmental Audit Committee Inquiry on Heatwaves:
techUK Response: Core Digital Infrastructure (data centres)

March 2018

Introduction

The Environmental Audit Committee Inquiry on our resilience to heatwaves is wide ranging but includes two specific questions relating to digital infrastructure: ***"What assessment has been made of the resilience of the UK's digital infrastructure to heatwaves?"*** and ***"To what extent has the Adaptation Programme taken account of this?"*** The scope of our response is to answer those two questions from the perspective of the UK data centre sector.

What is digital infrastructure?

Our core digital infrastructure is not a single system but multiple systems and networks that interoperate. The three main constituents are fixed line telecommunications (made up of the high capacity and highly resilient core network plus the access network that runs from the exchanges to tens of millions of individual customer premises), mobile telecommunications (that interact with the core network but provide customer coverage through a cellular network) and data centres (that manage, transmit, process and store data for government, businesses, individuals and academia).

What is a data centre?

A data centre is a building (or self contained unit) used to house computing equipment such as servers along with associated components such as telecommunications, network and storage systems. A data centre is equipped with a guaranteed power supply and high bandwidth connectivity. Resilience is critical so redundancy (duplication) of networks, power and other infrastructure is common to ensure continuity. Building management controls such as air conditioning maintain the environmental conditions for the equipment within a specified envelope of temperature and humidity, and security systems ensure that the facility and its data remain secure.[1]

We estimate that there are between 300 and 500 data centres in the UK, depending on definitions. 150-200 of these are colocation (commercial) facilities, operated by specialist data centre service providers. These include our very largest facilities. The rest are known as enterprise, which loosely means "in house" and they underpin corporate IT functions for all sorts of organisations like universities, banks and supermarkets. Sizes vary but on average these facilities are smaller. Many organisations use a mixture of outsourced and in house provision to minimise costs and risk.

What is special about digital infrastructure in an adaptation context?

Digital infrastructure has characteristics that make it relatively resilient to climate change: asset life is relatively short so more resilient assets can be deployed as part of the natural replacement cycle, there is built-in redundancy in IT infrastructures and technology development is fast and often able to innovate around threats. On the other hand the sector is highly dependent on energy and we are all increasingly dependent on digital infrastructure for our economic and social wellbeing, as this internet meme on Maslow's hierarchy of needs suggests.

[1] For more detail see "Er What is a Data Centre?"

Q1: What assessment has been made of the resilience of the UK's digital infrastructure to heatwaves?

techUK reported[2] on the readiness of our core digital infrastructure for climate change risks in 2016 having been invited by DEFRA under the Adaptation Reporting Power (second round). Our submission focused primarily on data centres but included information on telecommunications infrastructure where pertinent (and available). The most pressing climate change risk for data centres is flooding. Sustained periods of high heat were covered in the report but in truth this risk sits some way down the pecking order.

What are the risks?

Key climate change risks for digital infrastructure are summarised in the table in Annexe A, which includes heatwaves (listed as sustained high temperatures). In principle, heatwaves challenge the ability of a facility to maintain correct operating temperatures. Higher temperatures can cause equipment to overheat and components may fail, both within the IT hardware and the supporting networks and other infrastructures. Higher temperatures and humidity can shorten the life of hardware, increase the likelihood of degradation and negatively affect reliability. Heatwaves are likely to make working conditions less comfortable and could affect staff wellbeing if not adequately managed, increasing the risk of heat stress or even heatstroke. Heat stress leads to exhaustion, dehydration and impairs cognitive function and decision making. Heat stress also exacerbates existing medical conditions and is particularly problematic for older workers.

In practice, data centres operate reliably all over the world, from Singapore to Dubai: they are not in any way restricted to high latitudes or cool climates. The main by-product of computer processing is heat; controlling temperature is therefore part of standard operating procedure for data centres. Heatwaves essentially escalate the existing requirement. Moreover, rapid technology development and relatively short asset life provide opportunities for operators to improve resilience. Nevertheless, vulnerability to heatwaves is likely to be very mixed across the sector: in modern data centres the main challenge is likely to be the cost of additional cooling. In old or badly designed facilities there is a risk that functionality may be compromised.

Modern, purpose built data centres like those operated by commercial third party providers are well placed to deal with heatwaves for a range of reasons, including design and operational standards, service level agreements, cooling and server technology developments and reputational drivers. We will look at these factors in turn. Then we will consider parts of the sector where the picture may be more mixed.

Industry standards

Data centre design, build and operation are guided by well established international standards[3] that take into account climate extremes. Data centre design tends to be matched to function, so a mission critical facility will be designed and operated with resilience as the primary priority. Relevant design standards include EN 50600 Availability Classes, which run from 1-4 (4 being the most resilient). A Class 4 facility would have dual cooling capacity (200% of the maximum predicted requirement). Uptime Tier ratings impose similar requirements. Cooling capability can become a problem when a site is functioning close to, or at, capacity: critical national infrastructure sites are generally run below capacity for this and other reasons.

Cooling technology developments

Purpose built facilities deploy sophisticated air or water based cooling mechanisms that adjust automatically to ensure that ambient temperature and humidity remain suitable for reliable server function. Facilities can also take advantage of recent developments in evaporative cooling technology where (simplistically speaking)

[2] See: http://www.techuk.org/images/ICT_ARP_response_to_DEFRA_2016.pdf

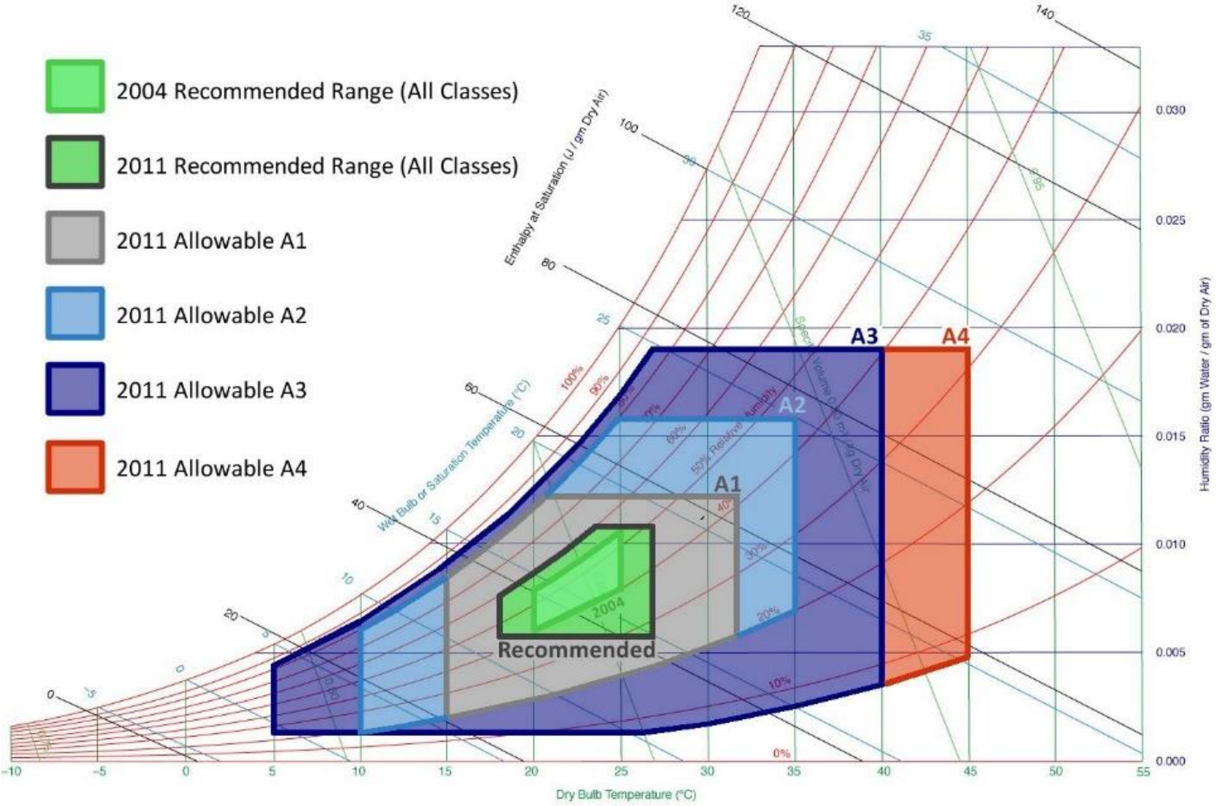
[3] Relevant risk related standards for data centres include: EN 50600 TR Availability Classes, ASHRAE, ISO 31000 , ISO 22301, Sarbanes Oxley, TIA ANSI 942 and BICSI ANSI 002 2014. The Uptime Institute's Tier rating system is a commercial design standard.

moisture is used to reduce air temperature. Evaporative cooling is effective at stabilising temperatures in the UK, where ambient humidity is relatively low.

Server technology developments

The most significant impact for modern, purpose built data centres will probably be the cost of additional cooling (cooling is more expensive per degree of temperature change than heating), which in turn could impact competitiveness, especially in regions like the UK where energy costs are relatively high. However, the industry has to some extent already envisaged this: the high cost of cooling has driven server manufacturers to develop devices that operate reliably at higher temperatures and humidity. The American Society of Heating, Refrigeration and Air Conditioning Engineers (ASHRAE) have expressed these ranges as operating envelopes. Manufacturers now warrant equipment up to ASHRAE-defined thresholds.

ASHRAE psychrometric charts like this one are familiar to the industry. If a server is warranted to a given ASHRAE level then it will perform reliably within the temperature and humidity envelope indicated in the diagram[4]. Recommended ranges are for continuous running and allowable ranges are for short term operation only. In fact, servers can work reliably at greater extremes but as the envelope widens, other components in the data centre may fail, there are diminishing returns in terms of efficiency and other negative impacts. Moreover, such conditions are unsuitable for staff working in the data halls. Allowable ranges are relevant to a climate change scenario because they enable operators to cope with heatwaves of limited duration without compromising equipment, or periods when part of the cooling infrastructure fails temporarily.



Asset life

Digital infrastructure is characterised by very variable asset life and this can be an advantage when preparing for climate change risks. Servers are designed for a life of around 5-7 years but they (or at least the central

[4] The expanded operating envelopes enabled by the work of ASHRAE means that even in relatively hot climates, mechanical cooling can now be minimised or avoided altogether. This demonstrates that warmer temperatures can be accommodated comfortably within normal operational practice. See the Green Grid map in Annexe 3 for an explanation.

processing units) should be replaced more regularly[5]. This presents an opportunity to deploy more resilient devices that can operate at higher temperatures as described above. Cooling systems have perhaps a 10-15 year life expectancy so again the technology refresh rate has the capability of remaining one step ahead.

Service level agreements, reputation and reporting

The commercial data centre sector trades on its reputation to provide resilience and security and therefore risk management is a very high priority. For organisations like banks where the business activity is underpinned by the data centre, the situation is similar. Many operators, both commercial and in-house, work to service level agreements with external or internal customers and are incentivised by the threat of penalties to monitor and manage potential risks and invest in mitigating measures. In general, while modern, purpose built data centres are not immune, these are not the type of facilities where climate change risks such as heatwaves are most likely to be most problematic.

Staff wellbeing

The Health and Safety Executive requires that working temperatures within buildings are "reasonable". Data halls, however, are classified as industrial facilities by the Code of Conduct for Energy Efficiency in Data Centres[6]. This explicitly states that engineers may need to enter hotspots and hot aisles for limited periods of time to ensure reliable facility function. Setting fixed thresholds of temperature and humidity would be unhelpful in this context and operators manage these situations through corporate risk assessments. We have consulted the sector and to date have received no reports of problematic working conditions within data centres or any record either formal or anecdotal of heat stress or heatstroke. However, we will keep asking. It is in operators' interests to ensure that temperatures in data centres are maintained at levels that are not problematic for staff, that periods of high temperature and humidity are short lived, and that operators ensure that staff working in these environments are given regular breaks and the opportunity to remain hydrated.

Potential vulnerabilities

Legacy (older) data centres, especially those that are close to or at capacity, are likely to be most at risk because their cooling systems will be challenged by sustained high temperatures. In addition, facilities with older cooling equipment may find it is inadequate to handle extreme temperatures, especially if sustained over days or weeks. At a device level, older servers that do not meet current ASHRAE standards are more likely to fail at high temperatures and humidity. Sites that have not adopted approaches like hot/cold aisle containment, hotspot detection[7] and other heat management technologies are also more likely to be at risk. Older facilities are unlikely to have been built to modern design standards and can be tricky to retrofit. There will be some sites that are simply badly designed and these too will be vulnerable.

Evidence from projects like EURECA (see below) and from anecdotal reports suggests that the more vulnerable data centres are likely (though not exclusively) to be found in-house, either within businesses or the public sector. Our concern is that there is little transparency regarding the operation of many of these sites, which are not accountable to customers and regulators in the way that commercial sites must be. The most likely scenario is a wide spectrum in terms of operational good practice and risk management. We do not have a clear picture of the state of readiness within this cohort of facilities. On the plus side they are less likely to be classed as critical national infrastructure[8] or to have wide-reaching mission critical functions.

[5] Servers operate 24/7 so the use phase dominates their life cycle energy use. Rapid improvements in processor efficiency means that severs should be replaced regularly to optimise energy efficiency. Working out how frequently this should be done can be complex but useful studies exist such as this one: http://ieeexplore.ieee.org/document/8263130/

[6] See: https://ec.europa.eu/jrc/en/energy-efficiency/code-conduct/datacentres section 5.3, pages 27-29 of the 2017 version.

[7] Heat is not distributed evenly throughout a data centre and there is a tendency for hotspots to develop. These have to be addressed either by reducing overall temperatures or by targeted management.

[8] If they were so deemed, additional resilience requirements would be placed on them.

Distributed IT

This is the part of our digital infrastructure that sits below the radar. Servers are held in cupboards and server rooms on office premises. We do not class these facilities as data centres but they should be included in any consideration of risk because this kind of computing supports a wide range of IT functions. Moreover, although the trend is towards outsourcing to cloud services or third party providers, we estimate that there are still thousands of these small facilities across the UK. This is borne our by findings from the recent EURECA project[9], tasked with helping public bodies improve the efficiency of their data centres, which reviewed 350 public sector facilities across Europe. Over 80% of these were very small, with fewer than 25 racks (which means that they are in reality server rooms and not genuine data centres), 40% of the servers in operation were over five years old (and therefore unlikely to meet current ASHRAE standards). Anecdotal reports from several sources suggest that operational efficiency is also very v ariable, service level agreements are not routinely in place, there is no systematic obligation to report outages, failures or near misses and in many cases the operational costs are not transparent. We take the view that this part of the UK's digital infrastructure may be less able to anticipate, manage and mitigate the risk of heatwaves.

Industry activity: summary

The sector continues to be fully involved with the Adaptation Programme, working formally and informally with DEFRA and the Environment Agency. Operators make use of a range of design and operational standards. Technology development is improving hardware resilience and cooling functions. Awareness of climate change risks is improving. A new initiative analysing the causes of data centre failures (DCIRN[10]) will reveal whether heatwaves are already impacting sector reliability. Staff wellbeing will continue to be a priority in managing these risks.

Q2 "To what extent has the Adaptation Programme taken account of this?"

We can provide a limited perspective on this question from our position as one of many infrastructure operators engaging in this programme. In general, the regular requirement to report on sector readiness drives us to review our progress and by doing so we build understanding and raise awareness within the sector.

We consider that the Adaptation Programme has accommodated the risk of heatwaves in its planning and risk assessments. The Programme has formally identified a series of risks under the CCRA and these have been assessed, categorised and tabulated. Drought and extreme heat are both included in this list. Both these risks have been classified as being relevant to digital infrastructure and are therefore included in the extract (see the table in Annexe B) that is being used as a basis for reporting by digital infrastructure sectors.

DEFRA is taking steps to encourage infrastructure operators to adopt a more systematic and standardised approach to adaptation reporting. We will be invited to use a template approach for reporting, which will standardise responses, allow the CCC's Adaptation Sub-Committee to track progress better and also help to ensure that operators are considering the full suite of risks.

The Environment Agency facilitates a forum for infrastructure operators to exchange information and work with others in the adaptation field. This is widely regarded as useful and productive and techUK participates.

Contact: Emma Fryer, Associate Director T: 01609 772 137 M: 07595 410 653 e: emma.fryer@techuk.org

About techUK: techUK is the trade association representing the digital technology sector in the UK. The tech industry is creating jobs and growth across the UK. In 2015 the internet economy contributed 10% of the UK's GDP. 900 companies are members of techUK. Collectively they employ more than 800,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium sized businesses. www.techuk.org

[9] See https://www.dceureca.eu/ The 2018 workshops presented lessons learned and findings from the work done in 350 public sector data centres across Europe. See: https://www.dceureca.eu/?page_id=4795

[10] Data Centre Incident Reporting Network, see: www.dcirn.org

ANNEXE A:

Extract from techUK's ARP Report, December 2016. Summary of climate change risks relevant to digital infrastructure

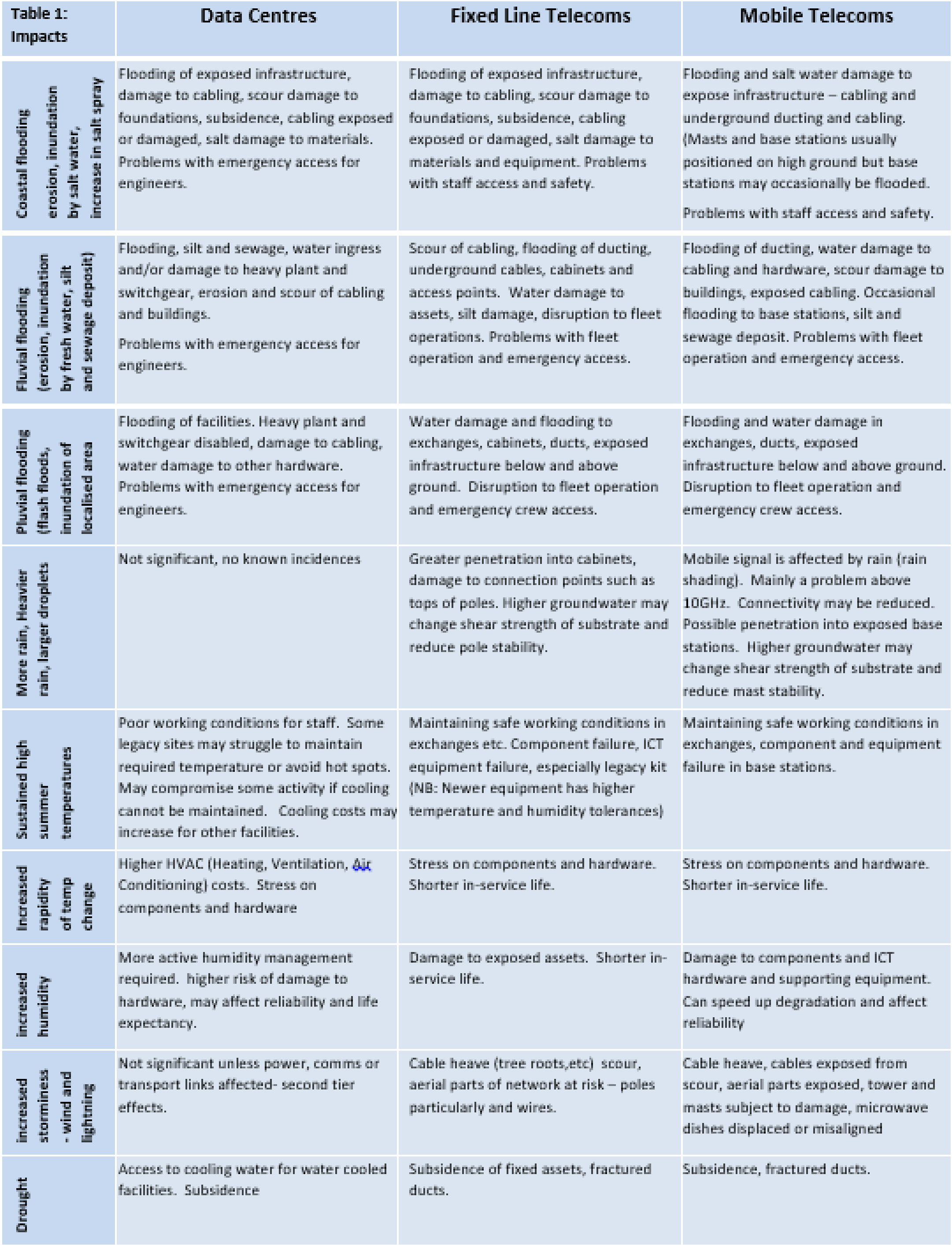
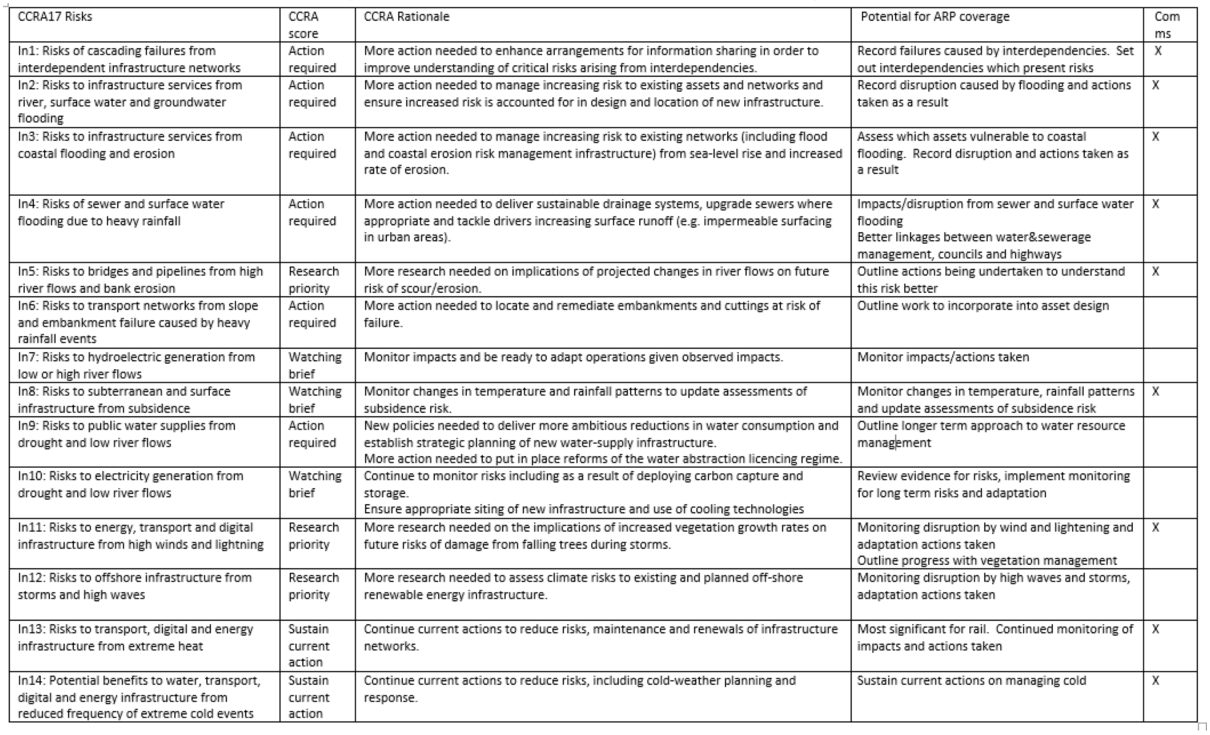


Table 1: Impacts	Data Centres	Fixed Line Telecoms	Mobile Telecoms
Coastal flooding erosion, inundation by salt water, increase in salt spray	Flooding of exposed infrastructure, damage to cabling, scour damage to foundations, subsidence, cabling exposed or damaged, salt damage to materials. Problems with emergency access for engineers.	Flooding of exposed infrastructure, damage to cabling, scour damage to foundations, subsidence, cabling exposed or damaged, salt damage to materials and equipment. Problems with staff access and safety.	Flooding and salt water damage to expose infrastructure – cabling and underground ducting and cabling. (Masts and base stations usually positioned on high ground but base stations may occasionally be flooded. Problems with staff access and safety.
Fluvial flooding (erosion, inundation by fresh water, silt and sewage deposit)	Flooding, silt and sewage, water ingress and/or damage to heavy plant and switchgear, erosion and scour of cabling and buildings. Problems with emergency access for engineers.	Scour of cabling, flooding of ducting, underground cables, cabinets and access points. Water damage to assets, silt damage, disruption to fleet operations. Problems with fleet operation and emergency access.	Flooding of ducting, water damage to cabling and hardware, scour damage to buildings, exposed cabling. Occasional flooding to base stations, silt and sewage deposit. Problems with fleet operation and emergency access.
Pluvial flooding (flash floods, inundation of localised area	Flooding of facilities. Heavy plant and switchgear disabled, damage to cabling, water damage to other hardware. Problems with emergency access for engineers.	Water damage and flooding to exchanges, cabinets, ducts, exposed infrastructure below and above ground. Disruption to fleet operation and emergency crew access.	Flooding and water damage in exchanges, ducts, exposed infrastructure below and above ground. Disruption to fleet operation and emergency crew access.
More rain, Heavier rain, larger droplets	Not significant, no known incidences	Greater penetration into cabinets, damage to connection points such as tops of poles. Higher groundwater may change shear strength of substrate and reduce pole stability.	Mobile signal is affected by rain (rain shading). Mainly a problem above 10GHz. Connectivity may be reduced. Possible penetration into exposed base stations. Higher groundwater may change shear strength of substrate and reduce mast stability.
Sustained high summer temperatures	Poor working conditions for staff. Some legacy sites may struggle to maintain required temperature or avoid hot spots. May compromise some activity if cooling cannot be maintained. Cooling costs may increase for other facilities.	Maintaining safe working conditions in exchanges etc. Component failure, ICT equipment failure, especially legacy kit (NB: Newer equipment has higher temperature and humidity tolerances)	Maintaining safe working conditions in exchanges, component and equipment failure in base stations.
Increased rapidity of temp change	Higher HVAC (Heating, Ventilation, Air Conditioning) costs. Stress on components and hardware	Stress on components and hardware. Shorter in-service life.	Stress on components and hardware. Shorter in-service life.
increased humidity	More active humidity management required. higher risk of damage to hardware, may affect reliability and life expectancy.	Damage to exposed assets. Shorter in-service life.	Damage to components and ICT hardware and supporting equipment. Can speed up degradation and affect reliability
increased storminess - wind and lightning	Not significant unless power, comms or transport links affected- second tier effects.	Cable heave (tree roots,etc) scour, aerial parts of network at risk – poles particularly and wires.	Cable heave, cables exposed from scour, aerial parts exposed, tower and masts subject to damage, microwave dishes displaced or misaligned
Drought	Access to cooling water for water cooled facilities. Subsidence	Subsidence of fixed assets, fractured ducts.	Subsidence, fractured ducts.

ANNEXE B:

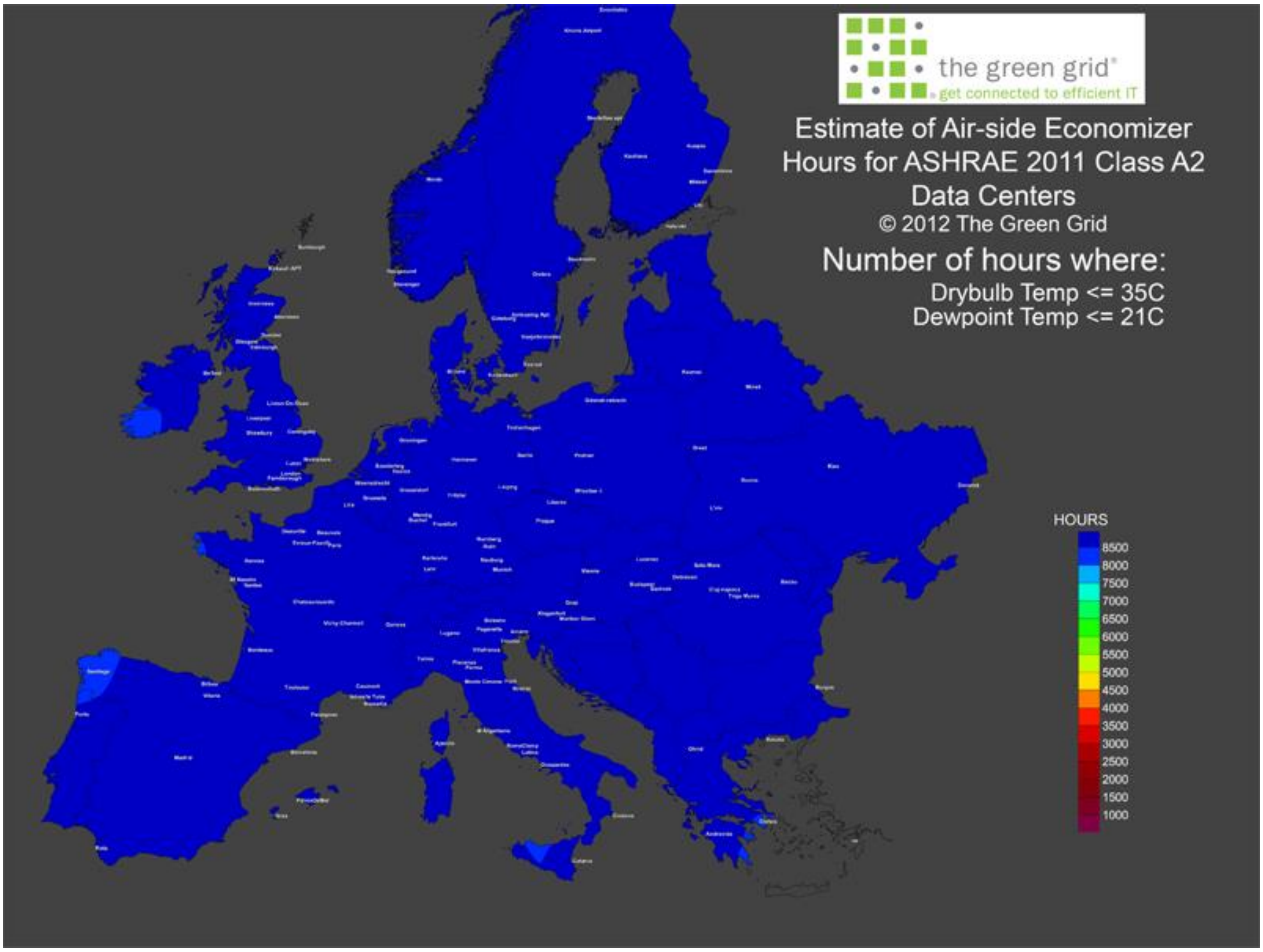
Table of CCRA (Climate Change Risk Assessment) risks relevant to digital infrastructure



CCRA17 Risks	CCRA score	CCRA Rationale	Potential for ARP coverage	Comms
In1: Risks of cascading failures from interdependent infrastructure networks	Action required	More action needed to enhance arrangements for information sharing in order to improve understanding of critical risks arising from interdependencies.	Record failures caused by interdependencies. Set out interdependencies which present risks	X
In2: Risks to infrastructure services from river, surface water and groundwater flooding	Action required	More action needed to manage increasing risk to existing assets and networks and ensure increased risk is accounted for in design and location of new infrastructure.	Record disruption caused by flooding and actions taken as a result	X
In3: Risks to infrastructure services from coastal flooding and erosion	Action required	More action needed to manage increasing risk to existing networks (including flood and coastal erosion risk management infrastructure) from sea-level rise and increased rate of erosion.	Assess which assets vulnerable to coastal flooding. Record disruption and actions taken as a result	X
In4: Risks of sewer and surface water flooding due to heavy rainfall	Action required	More action needed to deliver sustainable drainage systems, upgrade sewers where appropriate and tackle drivers increasing surface runoff (e.g. impermeable surfacing in urban areas).	Impacts/disruption from sewer and surface water flooding Better linkages between water&sewerage management, councils and highways	X
In5: Risks to bridges and pipelines from high river flows and bank erosion	Research priority	More research needed on implications of projected changes in river flows on future risk of scour/erosion.	Outline actions being undertaken to understand this risk better	X
In6: Risks to transport networks from slope and embankment failure caused by heavy rainfall events	Action required	More action needed to locate and remediate embankments and cuttings at risk of failure.	Outline work to incorporate into asset design	
In7: Risks to hydroelectric generation from low or high river flows	Watching brief	Monitor impacts and be ready to adapt operations given observed impacts.	Monitor impacts/actions taken	
In8: Risks to subterranean and surface infrastructure from subsidence	Watching brief	Monitor changes in temperature and rainfall patterns to update assessments of subsidence risk.	Monitor changes in temperature, rainfall patterns and update assessments of subsidence risk	X
In9: Risks to public water supplies from drought and low river flows	Action required	New policies needed to deliver more ambitious reductions in water consumption and establish strategic planning of new water-supply infrastructure. More action needed to put in place reforms of the water abstraction licencing regime.	Outline longer term approach to water resource management	
In10: Risks to electricity generation from drought and low river flows	Watching brief	Continue to monitor risks including as a result of deploying carbon capture and storage. Ensure appropriate siting of new infrastructure and use of cooling technologies	Review evidence for risks, implement monitoring for long term risks and adaptation	
In11: Risks to energy, transport and digital infrastructure from high winds and lightning	Research priority	More research needed on the implications of increased vegetation growth rates on future risks of damage from falling trees during storms.	Monitoring disruption by wind and lightening and adaptation actions taken Outline progress with vegetation management	X
In12: Risks to offshore infrastructure from storms and high waves	Research priority	More research needed to assess climate risks to existing and planned off-shore renewable energy infrastructure.	Monitoring disruption by high waves and storms, adaptation actions taken	
In13: Risks to transport, digital and energy infrastructure from extreme heat	Sustain current action	Continue current actions to reduce risks, maintenance and renewals of infrastructure networks.	Most significant for rail. Continued monitoring of impacts and actions taken	X
In14: Potential benefits to water, transport, digital and energy infrastructure from reduced frequency of extreme cold events	Sustain current action	Continue current actions to reduce risks, including cold-weather planning and response.	Sustain current actions on managing cold	X

ANNEXE C

Because of the improved tolerance of IT equipment, modern data centres are increasingly able to adopt free cooling, where fresh air is circulated through the facility and the use of mechanical chillers is minimised or even avoided altogether. The Green Grid's Free cooling map identifies the areas where facilities should be able to adopt this approach. These areas extend to southern Europe and this suggests that the UK should be able to continue to adopt free cooling even in a climate change scenario.


the green grid®
get connected to efficient IT
Estimate of Air-side Economizer Hours for ASHRAE 2011 Class A2 Data Centers
© 2012 The Green Grid
Number of hours where:
Drybulb Temp <= 35C
Dewpoint Temp <= 21C
HOURS
8500
8000
7500
7000
6500
6000
5500
5000
4500
4000
3500
3000
2500
2000
1500
1000