DIGITAL INFRASTRUTURE
AND THE IMPACTS OF CLIMATE CHANGE

Risks from cybercrime and terrorists are in the news every day. What is not so well broadcast, however, are the risks that exist to operators from climate change. Here, Emma Fryer explores digital infrastructure in the context of climate change risks, aiming to present some indicators of the general state of readiness, to identify areas where greater scrutiny is needed and to stimulate discussion on how these risks should be managed looking ahead.

EMMA FRYER
The effect of climate change

Climate change adaptation is about coping with the consequences of global warming, by recognising that climate change is already happening, and building resilience to the impacts. This differs from climate change mitigation, which seeks ways to prevent or minimise climate change by reducing greenhouse gas emissions, or by sequestering carbon.

In a policy context, adaptation means continuing to enjoy our current quality of life in a changed climate by ensuring that the complex support systems that we rely on can still function adequately when climate change risks are realised. We have to make sure they are resilient to things like flooding, sustained high temperatures and rapid fluctuations in temperature or humidity in the same way that we try to make them resilient to other forms of interference such

What is our core digital infrastructure?

The 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 which runs from the exchanges to tens of millions of individual customer premises), mobile telecommunications (that interacts with the core network but provides customer coverage through a cellular network) and data centres (that manage, transmit, process and store data for government, businesses, individuals and academia). Satellite communications and navigation systems and broadcast networks also play very important roles in digital infrastructure and, although out of scope for techUK's first submission [3], will be included in future sector reports.

as theft, vandalism or terrorism. Adaptation does not mean we have to live in caves and eat bugs.

The economic and social activities that make up modern life depend on advanced physical infrastructure such as the electricity grid and distribution network, water supply and sewerage, transport and digital communications networks, to name a few. These systems don't work autonomously – they are heavily interdependent – so a failure in one type of infrastructure can lead to failures in others. Imagine how well water supply would work without energy to drive pumps and provide pressure, or how well air traffic control would work without digital communications.

Government initiatives

Traditional adaptation planning tended to focus on improving resilience in individual services and the Government, following the recommendations of the 2008 Pitt Review [1], has exercised its power under the Adaptation Reporting Power[1] to require a number of infrastructure sectors to report on their climate change readiness. Recently, however, much more attention has been given to interdependencies. These interdependencies are asymmetric and changing. They are asymmetric because sectors are not necessarily mutually dependent. They are changing because energy has traditionally been viewed as the sector on which all other sectors depend, but the growing dependence on digital technology for business processes and transactions, for public service delivery and for social activity, means that ICT is emerging alongside energy as a core enabling infrastructure for all economic activity. Indeed, as the energy generating model becomes more dispersed and interconnected even the energy sector's dependence on a reliable communications network will increase.

Government has certainly recognised that we are dealing with a complicated system of systems, not a number of discrete sectors. Policy makers have also, more recently (and perhaps rather belatedly), acknowledged the importance of digital infrastructure: DEFRA invited the ICT sector to report on its readiness for climate change risks in the latest round of reports under the Adaptation Reporting Power. At the same time, Ofcom was invited to cover communications, and indeed had reported previously in 2011 [2], under the first round of reporting.

The author was tasked with putting together the submission [3] for digital infrastructure. This explained and defined digital infrastructure in the UK (see side panel). It set out the kind of climate change risks that could affect digital services and how these impacts might be manifested. It listed the information sources that service operators had access to inform their resilience planning and identified some of the industry standards that are applicable within this context. It also made a number of observations on barriers to the development of adaptive capacity and on actions that could be taken to bridge knowledge gaps and to build awareness.

Mindful that the communications sector had already reported under a previous round, when it came to the more detailed aspects of readiness reporting the submission focused on the UK data centre estate, which was an element not covered elsewhere, or at least not explicitly. This also made sense from a pragmatic point of view: techUK is an industry association with the vast majority of the commercial (colocation) data centre sector in membership and a large proportion of the enterprise providers, especially IT services companies, so it is in a good position to report at sector level on behalf of that community. The submission also made observations on mobile telecommunications provision. Fixed line infrastructure is primarily delivered by one incumbent provider with its own well-developed corporate risk plan. Rather than second-guess the contents, the techUK submission limited itself to a general overview of the state of play. The important thing to remember is that this is a first submission in an iterative process, which it is envisaged will inform a more comprehensive appraisal in future.

Information about climate change and the risks

Climate change risks relevant to digital infrastructure include flooding from increased winter rainfall, higher winds and higher tidal ranges, changes to humidity and temperature, drought and increased storminess. UKCP09 (UK Climate Projections) [4] provide? the primary information source. The projections include probabilistic scenarios for rainfall, temperature and humidity that are relevant for future planning and standards development within the sector, although it is not clear that these are widely used by operators. The Environment Agency's "Flood map for planning" [5] provides localised flood risk information and is extensively used by operators, advisors, investors and consultants to inform decision making, especially choice of location and design. It is also revisited during the operational stage to meet bid requirements, for insurance renewals and to comply with availability standards, but regular review is not systematic across the industry. The extent to which the sector is aware of, and uses, other

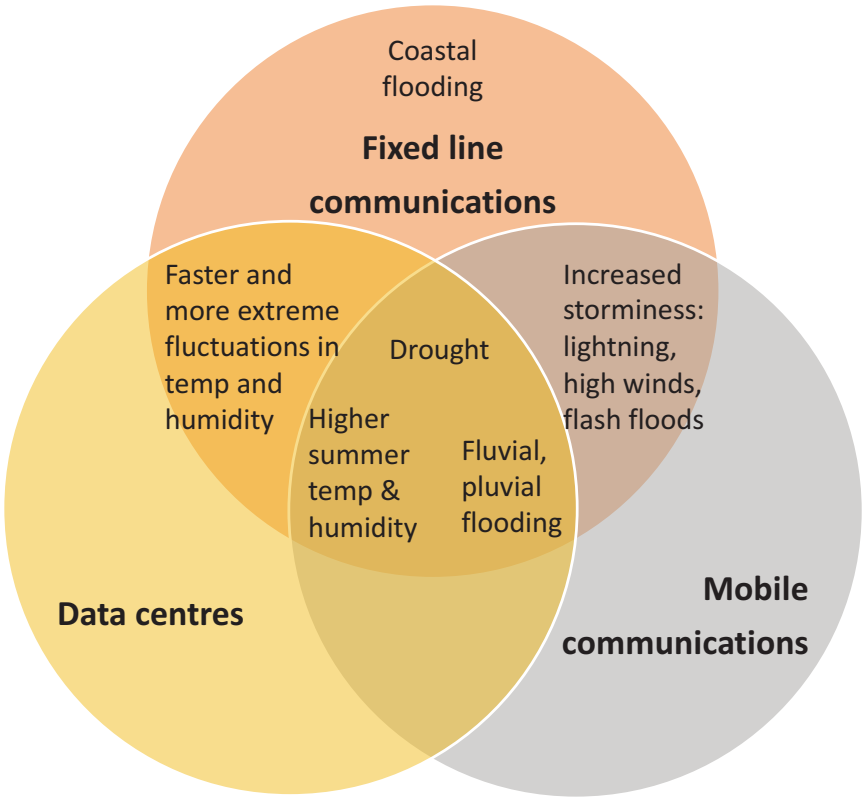

Figure 1: Overlap of the impact of climate change threats on the digital infrastructure.

Environment Agency data such as surface water modelling is variable.

Threats to the digital infrastructure

Digital infrastructure has some unique characteristics that make it relatively resilient to climate change: compared to other fixed infrastructure, average asset life is relatively short so more resilient assets can be deployed as part of the natural replacement cycle, there is more built-in redundancy in ICT 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 society as a whole is increasingly dependent on ICT for its economic and social wellbeing. The multiple interoperable systems that make up digital infrastructures confer advantages in terms of redundancy and overlap but they are also complex. Not all interdependencies are known and rapid changes in technology may expose the sector to new and unexpected vulnerabilities.

Climate change threats relevant to digital infrastructure include coastal, fluvial and pluvial flooding from increased winter rainfall, increased severity and frequency of storms (which means more lightning, more incidences of high winds, higher maximum wind speeds and more localised downpours with bigger droplets). We can also look forward to increased average summer temperatures and higher winter humidity, longer sustained periods of high temperature and high humidity, greater rapidity in temperature and humidity fluctuations, and drought. Statistical changes to the incidence of rainfall will affect the calculation of availability of service for wireless applications but the adaptation process is a manageable one. Figure 1 illustrates the overlap of the impact of these threats on the digital infrastructure.

Physical impacts include flooding of buildings, ducting and other assets; water, silt and salt damage, scour of cabling and foundations, subsidence to buildings and masts, problems of access for engineers and staff, disruption to fleet operations, cable heave from uprooted trees, lightning damage to poles and cables, wind damage to poles and masts, higher costs of cooling, stress on components, component failure, shorter asset life, reduced reliability, fractured ducts, reduced signal strength and higher operating costs (for instance higher cooling costs for data centres in hot weather, obligation to boost signal strength, etc.).

Non-physical impacts include reputational damage, failure to meet customer service level agreements, failure to meet regulatory objectives, high customer call volumes, impacts on staff wellbeing and unbudgeted costs.

Managing climate change risks

Climate change risks are handled as just one of a myriad of business risks facing the sector, and are prioritised accordingly. Data centres, for instance, compete on the basis of resilience; resilience tends to be matched to criticality and to price so, the more important the data is, the more resilient the facility. This is usually achieved through "redundancy", which carries both capital and operational costs. As a broad rule of thumb, "you pay for what you get". The sector also makes use of a range of industry standards that, although not designed specifically with climate change risks in mind, provide auditable approaches for managing these risks. Data centre availability classes described under the EN 50600 [6] series of standards are a useful example. Data centres work to other generic risk standards such as ISO 31000 [7]. Operators adopt formal risk management tools and processes. Scenario planning for emergencies is common.

At build and design stage, flood is at the top of the list of risk factors when choosing a location for data centres and core network infrastructure; although there is no agreed risk threshold, industry practitioners generally seek a risk below 1 in 1000. This is, however balanced with other factors and emphasis is on managing and mitigating the risk rather than working to inflexible thresholds. Operational risk management is

not limited to physical protection and data centres may be mirrored to ensure a continuously available backup. Power availability is key and batteries provide instantaneous power in the event of a grid outage, with diesel generators for longer outages. Similar approaches are taken by communications providers for core network functions. As a rule of thumb, the more premises an exchange serves, the higher its resilience. Larger exchanges have battery and diesel backup, smaller exchanges may just have battery power suitable only for short term outages. In remote locations, small exchanges may run primarily from generators, so access for refuelling is the key constraint in those cases. In addition, communications providers follow recognised industry standards for the construction of masts and towers – BS 8100, EN 1991-1-4, EN 1993 and PLG07.

Barriers to developing adaptive capacity

Building adaptive capacity does not come cheap and making the business case for investing in something that may not be needed can be very tricky. However, cost is not the only barrier. There are interdependencies with other infrastructures; the sector relies heavily on electricity and to a lesser extent on transport (for regular operations, emergency access and generator replenishment in times of power outage), and on water. So ICT is not truly resilient unless the power supply is equally resilient. Digital services are also vulnerable to failures in physical "pinch points" like bridges that carry multiple utilities – communications, electricity and water. Within ICT there are also critical sub-sector interdependencies; data centres cannot function without communications and vice versa. The complexity of our digital infrastructure can sometimes make it difficult to understand and identify these interdependencies.

Other internal barriers include a mixed picture of awareness both regarding relevant information sources and how well climate change risks are understood. External barriers include a disproportionate policy focus on protecting physical assets rather than on business or service continuity. For communications' providers, there are circumstances in which regulatory approaches could have unintended consequences on resilience (such as the conditions of the fixed line Universal Service Obligation which could possibly take a more pragmatic approach to provision in flood risk areas) or the emphasis on driving competition around consumer prices within the mobile communications sector (which some observers feel could reduce funds for infrastructure investment). Sectors also report that, in price review negotiations, regulators can be unwilling to allow for long term investments because the benefits are not captured within the relevant price review period. Finally, an historic failure to enforce planning policy in flood zones has also been unhelpful, although techUK understands anecdotally that there is now greater scrutiny on such developments.

Learning from recent events

The UK's digital infrastructure has to date been relatively resilient to severe weather. While there have been isolated incidents and localised interruptions in service, the sector has not suffered the scale of problems encountered by other utilities, such as those experienced during the 2007 floods, which left tens of thousands of people without water and electricity. This is no reason for complacency. The sector has learned lessons and implemented changes following recent events including loss of communications services in York and Leeds in 2015 due to flooding in a telephone exchange and a network centre. However, the most serious events were abroad; hurricane Sandy impacted data centres in New York and New Jersey, and the sector has also learned from Japan where prior planning ensured that Japanese data centres escaped serious damage from the 2011 tsunami. Improvements have been implemented to fuel storage, switchgear protection, communications and emergency access arrangements.

Observations and recommendations

techUK's first report [3] to Government made some recommendations. These included suggestions for a more standardised approach to the climate change projections so that all sectors are using the same dataset, a policy approach that accommodates service delivery rather than just focusing on asset protection and a more robust approach to dealing with those flood plain developments that are at odds with Environment Agency advice. The report suggested a more proactive process for identifying single points of failure in physical infrastructure following incidents such as the bridge failures at Tadcaster and Cockermouth. It also hinted that a couple of regulatory aspects might be revisited to ensure that they do not result in unintended consequences that could hamper the sector's ability to build adaptive capacity. Although the sector is happy to provide bespoke reporting on its state of climate change readiness, techUK believes that climate change risks should continue to be handled as part of the wider risk portfolio within the ICT sector. Moreover, techUK does not see a need for these risks to be handled separately, or segregated from existing corporate risk management processes, which would probably add complexity and cost.

Future direction

The climate change adaptation agenda is only one of the many issues addressed by techUK's data centre programme and it sits some way down in the pecking order below issues such as energy costs, energy efficiency, regulatory and compliance burdens and competitiveness – plus the implications of Brexit on the sector, of course. However, techUK will continue to monitor any publicly reported events and share learning outcomes, raise awareness of the nature of climate change risks, the information available, and how it should be used. It will alert the industry to relevant standards and develop recommendations for operators to review flood risk regularly. techUK will continue to engage with external stakeholders and regulators and if there are further rounds of reporting, it will report.

Next steps

Looking ahead there are areas where tech UK can take a lead at sector level.
Reviewing flood risks – More data is needed

on how often operators re-examine flood risks; it is understood they do it but they are not always communicative and there is not yet a systematic means of gathering this information. Telecoms providers are familiar with handling climate change risks but they are less familiar with communicating their actions formally, or separating these risks from other business risks. This is what DEFRA's Adaptation Reporting Power seeks to address, and it is already becoming clear that a much more comprehensive picture of national preparedness will emerge over time.

Learning from events – The ICT sector has (fortunately!) a very limited evidence base of failures to inform future actions: an obvious paradox – we certainly do not want a larger catalogue of incidents... so it is important to learn as much as possible from the limited number of incidents that have occurred, from abroad and from events in other sectors that can provide useful proxies. techUK sits on the Infrastructure Operators Adaptation Forum, an informal but very useful group that meets three times a year to exchange information and raise relevant issues with policy makers.

Understanding interdependencies – Understanding of interdependencies needs to be improved. Some interdependencies are already clear; digital infrastructure is heavily dependent on energy, data centres are dependent on communications, communications run through physical pinch points like bridges. So these risks can be accommodated to some extent. But there are areas that are less clear: like data and voice traffic flows where single points of failure exist that are not fully recognised and where for instance the loss of a single mast, say a shared mast that is being used by multiple providers for access and backhaul, could have a more significant impact than anticipated. Understanding or being in a position to map these flows in any meaningful way in the short to medium term is unrealistic, and, in any case, they will change. However, efforts could be focused on trying to develop a better understanding of what is known and the extent of what is not known – or to use Donald Rumsfeld's terminology, to be better able to quantify the known knowns, the known unknowns and the unknown unknowns.

AUTHOR'S CONCLUSIONS

From techUK's perspective, this has been an exercise to try to understand digital infrastructure in the context of climate change risks, to present some indicators of the general state of readiness, to identify areas where greater scrutiny is needed and to stimulate discussion within the sector itself on how these risks should be managed looking ahead. The important thing is that operators are aware that climate change risks exist, that they have to be actively managed as part of the risk portfolio and that, just like risks from terrorism, they are constantly changing.

ABOUT THE AUTHOR

Emma Fryer, Associate Director, techUK currently leads the data centre programme for technology sector trade body techUK, providing advocacy on behalf of UK operators. She produces thought leadership, policy responses, white papers, briefings and infographics covering topics from generator emissions to Brexit. She also wrote the sector's climate change resilience report submitted to DEFRA. Emma is a recipient of two prestigious awards, is a regular speaker at industry events and now sits on several judging panels.

ITP INSIGHT CALL
Want to know more?
Join in the ITPInsight Call. Visit:
https://www.theitp.org/calendar/

REFERENCES

1. The Pitt Review – Learning lessons from the 2007 floods. Jun e2008. Available at: http://webarchive.nationalarchives.gov.uk/20100807034701/http:/archive.cabinetoffice.gov.uk/pittreview/thepittreview/final_report.html
2. Ofcom. Climate Change Adaptation - Impact on our functions. Sep 2011. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0031/56947/climate-change-adaptation.pdf
3. techUK. The UK's core digital infrastructure: Data centres climate change adaptation and resilience. Dec 2016. Available at: https://www.techuk.org/images/ICT_ARP_response_to_DEFRA_2016.pdf
4. UK Climate Projections (UKCP09). Available at: http://ukclimateprojections.metoffice.gov.uk/
5. Department for Environment, Food & Rural Affairs. Flood map for planning. Available at: https://flood-map-for-planning.service.gov.uk/
6. EN 50600 series of standards. Data centre facilities and infrastructures. Available via: http://shop.bsigroup.com/
7. ISO 31000 Risk management. Available via: https://www.iso.org/standards.html

FOOTNOTE

1 The Adaptation Reporting Power or ARP gave DEFRA the authority to require sectors to report on their readiness for climate change risks.

This emerged from the recommendations of the 2008 Pitt Review following the catastrophic 2007 floods which resulted in major failures in water and electricity provision in some locations.

The first reporting round was in 2011 and the second ended in 2016. More rounds are anticipated.