Government Office for Science

Foresight

Infrastructure and Resilience

Commissioned Review

Foresight, Government Office for Science

Contents

Infrastructure Resilience

Peter Guthrie and Thalia Konaris

27 November 2012

Report produced for the Government Office of Science, Foresight project ‘Reducing Risks of Future Disasters: Priorities for Decision Makers’

Introduction

The US Department of Homeland Security defines critical infrastructure, as *"the systems and assets, whether physical or virtual, so vital to the nation that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"* (Department of Homeland Security 2012). In the UK, infrastructure is divided into the nine sectors of food, energy, water, ICT, transport, health, emergency services, government and finance. Assets within these that have been identified by the Government to be of importance to basic service delivery and national security are collectively known as Critical National Infrastructure (CNI).

The UK is sustained by a highly complex and interconnected network of infrastructure systems. The value of its civil engineers works in 2010 was estimated at £790 billion and a further £250 billion is expected to be invested in the sector over the next decade and beyond (Frontier Economics 2012). The pursuit for infrastructure resilience requires a pursuit for the reduction of failure probabilities, reduction of negative consequences when failure does occur, and reduction in recovery time (Chang 2009; Walker *et al*. 2004). The importance of protecting this infrastructure from threat lies not only in its critical role of sustaining societies, but also in its role of helping communities and the economy to rebuild themselves post-disaster. Service disruptions caused by asset damage can lead to economic and societal impacts which, in the case of vulnerable groups, can be difficult to recover from.

Summer 2007 Floods

In 2007, the UK experienced prolonged floods which cost the UK economy over £4 billion, with damages to critical infrastructure estimated at £674 million, exposing the nation's vulnerability to natural threat (Cabinet Office 2011). The Mythe water treatment works flooded leaving 350,000 people with no clean water for up to 17 days, the Central Networks' Castle Meads electricity sub-station was shut down, leaving 42,000 people without power, some 10,000 people were left stranded on the M5 motorway, In Yorkshire, four major electrical sub-stations and 55 secondary sub-stations were flooded, affecting the supply to 130,000 people (Pitt 2007).

Following the recommendations of the Pitt Review for the development of a national standard for resilience against flooding, in 2009 the Government initiated the development of Sector Resilience Plans (SRPs) for each of the abovementioned nine sectors, in collaboration with regulators and industry. These are produced annually and are written in relevance to the risks identified in the National Risk Assessment (NRA) in which the government assesses every 5 years the likelihood and impact of civil emergencies including risk of terrorism, major accidents and natural hazards. Although individual plans are classified, an unclassified summary is released annually. SRPs present the risk and vulnerability of each sector, the desirable level of resilience, a programme of actions for achieving the desired level and methods of reporting on progress towards achieving it (Cabinet Office 2012a).

Due to size limitations, this report focuses primarily on the resilience of the energy, transport, water and ICT sectors as these employ large-scale physical assets, transport key resources nationally and link the UK internationally. The report draws from open-source material to discuss the nature of the risks posed to CNI, presents current barriers towards developing resilience, and offer recommendations for overcoming these based on emerging opportunities.

Risks to infrastructure

The complex nature of infrastructure is attributed to several factors including its interconnectedness, which will be elaborated on in subsequent paragraphs, its influence by geography, the weather, demography, the number and behaviour of its users, and technological innovation. Sources of threat to infrastructure can be categorised as:

1. External threat: including natural hazards; or threat from human conflict or crime

2. Threat caused by industrial activity: Organisational or equipment failure leading to major accidents; or long-term unsustainable practices

The risk of impact from these is dependent on their likelihood of occurrence and the severity of their impact. According to the National Risk Register, the unclassified version of the NRA, this likelihood, where possible, is determined based on historical data and modelling simulations – particularly for natural or accidental hazards. For crime or terrorist threat, likelihood determination is derived from an assessment of the willingness and capability of attack. The severity of consequences is measured through a combination of numbers of fatalities, illness or injury, levels of social disruption, economic harm and psychological impact(Cabinet Office 2012b).

As Climate Change adaptation and mitigation are gaining centre-stage on the global and national agendas, infrastructure resilience against natural hazards and extreme weather events is becoming increasingly important. According to the NRR the natural hazards most likely to cause a threat to the UK include coastal flooding, inland flooding, storms and gales, low temperatures and heavy snow, heat waves, drought and volcanic ash. As Table 1 highlights, mitigating these risks requires understanding of the interconnectedness between weather events and how natural hazards, like river flooding for example, can originate from entirely different weather patterns. The NRR also identifies non-climate related risks including major industrial accidents, malicious attack by criminal or terrorists including cyber attack, and infectious diseases of humans or animals.

Table 1: Interconnectedness of natural hazards (Cabinet Office 2011)

Source	Initial Consequences	Knock-on Consequences
Storms and Gales	Strong winds (Gales) Tidal surge Snow Lighting Heavy Rainfall Tornadoes Hail	River and coastal flooding Surface water flooding Land instability Wildfire
Prolonged period of hot weather (at least 5 consecutive days)	Heat	Thunderstorms Drought Dust/Smog/Haze Land instability Wildfire
Prolonged period of dry weather (developing over 3 years)	Reduced Rainfall	Dust/Smog/Haze/Fog Reduced ground water flow Water quality Land instability Drought Wildfire
Excessive cold with snow	Cold Snow	Ice Ice accretion Wind chill Fog Surface water and river flooding (snow melt)

According to DEFRA (2011), the threat to **energy infrastructure** assets and services is posed predominantly from increased precipitation, temperatures, frequency of storms and changes in wind. Flooding can damage fuel processing and storage facilities, hinder transportation of fuel, or disrupt power generation and energy distribution. Increased temperatures in turn can

decrease the efficiency of fossil fuel-power plants and the capacity for electricity distribution networks.

Stuxnet Software virus (2010)

Information systems controlling critical infrastructure such as oil, electricity, water and gas, have traditionally been closed, private and managed from single control centres. However, increased efficiencies earned by connecting control systems via the internet and cloud computing across utilities around the world is causing increasing cyber-vulnerability to cybercrime, data fraud/loss or Critical Information Infrastructure system failure, the WEF 2010 Global Risks Report warns (World Economic Forum 2010).

An example of one such threat is the Stuxnet Software Virus, which was discovered in 2010 and identified as the first virus designed to target industrial infrastructure, such as power stations. The predominant target of the virus was discovered to be Iran's nuclear program, specifically 5 industrial processing organisations, the work of which was delayed by two years as a result, and is suspected to be the cause of setback to Iran's uranium enrichment program. The worm was designed to seek out Siemens industrial control software, and overwrite existing instructions of industrial machinery. It has been described as *"one of the most sophisticated pieces of malware ever"*, damage from which *"could cause another Chernobyl nuclear disaster"*. Nonetheless, the recently discovered Flame virus, which is found to contain components of Stuxnet and is targeting the petroleum industry, is said to be even more sophisticated (Fildes 2011).

Due to their geographical spread and exposure, **transport infrastructure** assets and services are most vulnerable to increased storms and flooding. Bridges, roads and infrastructure can experience damage due to flooding and increased river flow. Wet winters and dry summers can damage road embankments while underground trains can overheat during periods of high temperature. Ports and airports can be threatened by high tides, storm surges and high winds.

Water infrastructure assets and services are at risk predominantly from extreme weather events and changes in precipitation. While periods of drought can reduce security of water

supply and increase contamination, periods of heavy rainfall can cause increased river and sewer flooding.

The UK's **ICT infrastructure** is becoming increasingly important as communication within social, economic, and industrial systems is becoming increasingly digital. It is the nation's perhaps most internationally interconnected infrastructure and while physical infrastructure may be hosted locally, data transfer and storage may take place internationally. From a resilience perspective, while this can offer additional capacity and data security in the likelihood of local disruption, it can also make UK infrastructure vulnerable to entirely different natural and human threats that other nations are vulnerable to.

In the UK, extreme weather events and rainfall can flood underground ICT infrastructure, damage over-ground infrastructure and prevent access to damage sites for repair particularly in the case of heavy snowfall. Yet, it is during such events that demand for ICT services can increase as people conduct business remotely or contact family during emergencies. Increasing temperatures are likely to cause overheating in data centres and base stations and influence the distance wireless signals can transmit. While changes to precipitation and humidity can affect the ability of wireless devices to pick up signals.

Lastly, all NCI, and particularly ICT infrastructure, is reliant on imported materials, including so-called critical rare-earth metals, which are becoming increasingly important as the UK shifts to a low-carbon economy. The US Critical Materials Strategy outlines 14 such materials which will become critical in terms of their importance to the economy but also their availability. Examples include Cobalt and Lithium which are vital for use in lithium ion batteries for use in electric vehicles, cell-phone, tablet and laptop technologies. Availability of critical materials can hinder production of solar cells, energy efficient lighting, wind turbines over and above current uses (US Department of Energy 2011).

Infrastructure Interdependence

Early efforts for increasing infrastructure resilience have focussed on using increasingly accurate tools to predict the intensity of natural hazards and engineer components that can withstand the newly predicted shocks. However, as the complex impact of service interruptions on dependent infrastructure, society and business have become more apparent, enquiry has

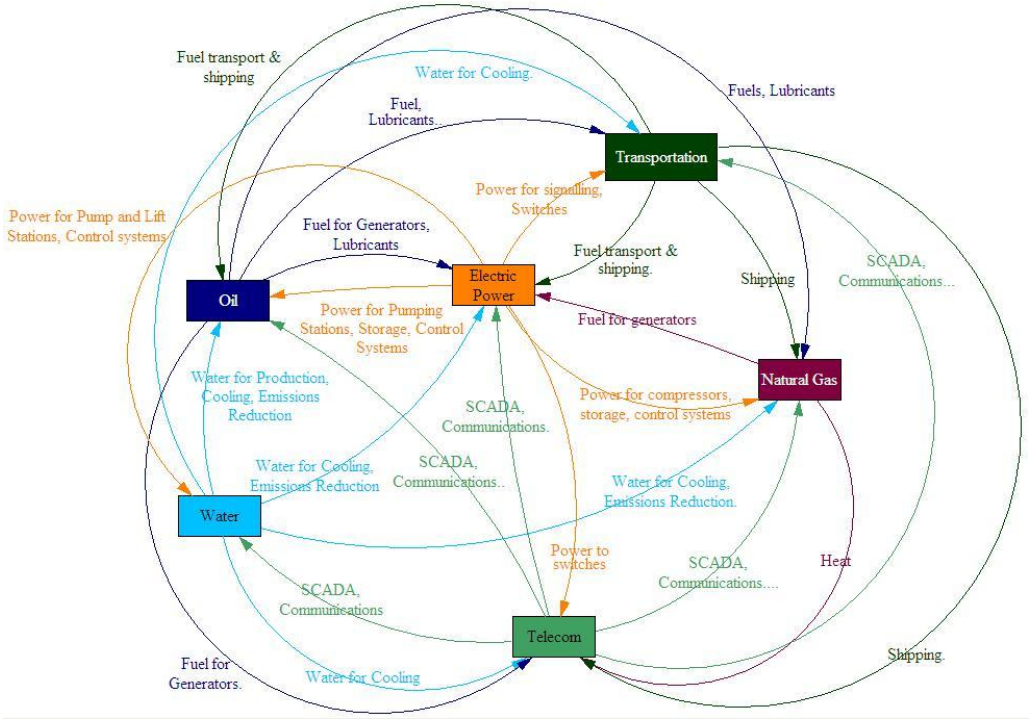
become more multidisciplinary to explore interdependencies within infrastructure systems and with society and economy (Chang 2009). The centralised nature of urban infrastructure and the interconnectedness between services implies that damage at a point in the system can have knock-on effects through that and other infrastructure systems.

> In August 2003 a power outage in northern Ohio caused the largest blackout in the history of North America, affecting parts of Northeastern and Midwestern United States and Ontario Canada. Over 508 generators and 265 power plants were shut down, leaving 55 million people without power and affecting amongst others, water supply, telecommunications and transportation. The failure cost $10 billion in losses (Natural Resources Canada 2006).

UK infrastructure is highly interconnected and is also linked with infrastructure in other countries. It has long been recognised that understanding these interconnections will help identify points of critical vulnerability. In their study of catastrophic cascade of failures in interconnected systems, Buldyrev *et al*. conclude that while in an isolated single network a significant number of network nodes must be removed (representing components or systems failing) for the network to break down, when dependencies between networks are taken into account, removal of only a small fraction of nodes can result in fragmentation of the entire system. This highlights that system interdependency can increase the vulnerability of individual systems (Buldyrev *et al*. 2010).

Figure 2 presents the primary ways in which the Oil, Gas, Water, Electric power, Telecoms and Transport industries are interdependent in terms of input materials and services. As can be seen in Figure 1, ICT infrastructure is perhaps the most interconnected with other UK systems on multiple levels, and its use for making operations more efficient and productive, is expected to increase. However, a risk can emerge where increasing reliance on ICT to increase efficiency can lower the case for development of additional physical capacity. This can decrease resilience of such systems which operate closer to full capacity, and are vulnerable in the case of ICT failure. Nonetheless, advances in IT have now allowed huge steps forward in decentralised control of networks.

Figure 1 Interdependence between critical infrastructure systems (Little 2002)



Infrastructure interdependence can be grouped into:

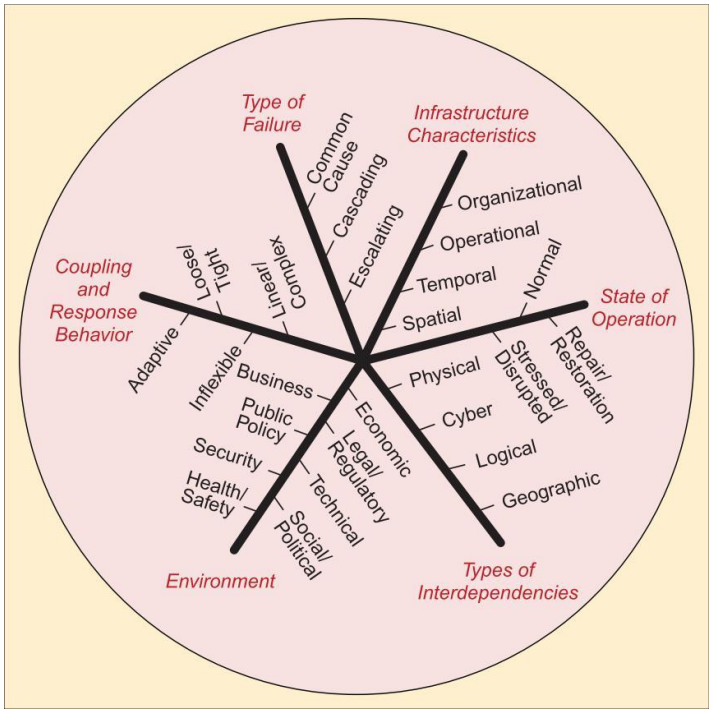
- **Regional convergence** (aka **single point**): refers to a convergence of critical infrastructure components through a specific geographical location

- **Cascade failure:**
  - **Inter-system:** where failure in one infrastructure system causes failure in one or more interconnected infrastructure systems.
  - **Intra-system:** where failure within an infrastructure system impacts later stages of operation within the same system

Therefore interdependence can be brought about due to the physical proximity of systems or due to their operational interdependence. Figure 2 presents a framework developed by Rinaldi *et al* (2001) which enables the characterisation of interdependence between two infrastructure systems according to the environmental factors, the nature of their connectivity and the current state of operation of each system. Pederson *et al*. suggest the additional consideration of policy or procedural interdependency where a policy within or external to a system relates to an event change that impacts another system, and also the consideration of societal interdependency (Pederson *et al*. 2006).

Using Figure 2, vulnerability can become maximised under a scenario where a system is under stress, where it is tightly and non-linearly connected to other systems such that cascading and potentially escalating influence on these is inevitable, and when the connection exists on multiple levels, both virtual and physical, in an external environment of multiple pressures from regulatory, economic and social systems. Similarly, indirect impact on a system from another can be minimised by ensuring that their connection is kept loose and adaptive. One way of ensuring this practically is to ensure that systems are reliant on multiple rather than a single input or output route for a certain function, such that if one fails, others can be utilised. Adaptive mechanisms are discussed further in subsequent paragraphs.

Figure 2. Dimensions of Infrastructure Interdependence (Rinaldi *et al*. 2001)



Barriers to Resilience

In a recent report, the Council for Science and Technology highlights that UK infrastructure currently has major vulnerabilities, requiring a complete shift in trajectory if a resilient future is to be ensured (Council for Science and Technology 2009). The long life-span of critical assets has led to a presently fragmented, ageing infrastructure network which suffers from lack of overall regulation and vision, a lack of a clear understanding of interdependencies, and a lack of overall accountability. Investment is focussed on replacing and renewing rather than modernising infrastructure and expenditure takes place in response to a crisis rather than proactively. Furthermore, due to economic and social pressures, today's infrastructure is operating at near maximum capacity and is not future-proofed against anticipated climatic and socio-demographic changes.

These vulnerabilities form a challenge particularly with regards to **Climate Change adaptation**. They imply that planning of infrastructure development is fragmented and relatively short-term compared to the lifespan of its assets, thus discouraging consideration of climatic change impacts expected to occur during that lifespan. Instead climatic changes are adjusted-to incrementally through a reactive rather than proactive, systemic approach (DEFRA 2011). However the interdependent nature of infrastructure implies that while climate change preparedness at a point within the system might be more evolved than in others, it is still vulnerable to failure caused at other, less resilient points.

Furthermore, uncertainty, long pay-back times and financial risk involved in resilience investment can discourage the latter. In an **increasingly privatised infrastructure sector**, regulation which enforces considerations of long term impacts and investment in long-term resilience, rather than putting emphasis on short-term value for money, is crucial. A low carbon, resilient future is currently very much in the hands of the private sector and appropriate market signals are needed to ensure it progresses uniformly.

As mentioned in section 2, organisations' **drive for efficiency**, fuelled by competition and socio-economic pressures, can increase quality of service, but can compromise resilience and flexibility. In other words, while organisations are competing with each other, they can undermine their inherent dependence on the success of their competitors (or lack of failure).

There is a challenge therefore, of balancing adaptation and resilience priorities with other often conflicting priorities at a strategic level of organisations.

The sector also suffers from a **lack of relevant, timely information** tailored to stakeholders, on vulnerabilities within and between infrastructure sectors. If an organisation is not accountable for the impact of their activities on another, it may have little incentive to communicate internal information on resilience and threat to their own facilities. Recognising this, the Government's initiative to enforce the development of Sector Resilience Plans is a step forward towards making sectors accountable to each other and to the public. Even if willingness or obligation is in place for information-sharing, there is still a gap in understanding how infrastructure systems influence and are influenced by each other, the wider society and the economy. Subsequent paragraphs will discuss current effort in interdependency modelling in simulation.

The sector is governed by a variety of standards none of which, however, address resilience, response and recovery directly. **Design standards** are aimed at ensuring the physical integrity of the asset within the range of environments it will be exposed to, rather than the integrity of the service. While **network design standards** take resilience into consideration through spare capacity and re-routing options, this is more feasible in sectors like electrical distribution systems, and less feasible in the water or transport sectors owing to the cost of redundancy and operating at near full capacity. **Service standards** are intended to provide customers with confidence in the quality, safety and reliability of the service being provided, and hence do encourage the development of resilience against service interruptions. However, they do often include exception clauses for extreme weather events or unexpected operating conditions. Furthermore, penalties payable to customers for loss of supply do not necessarily reflect the actual cost or inconvenience to the customer (Cabinet Office 2011).

Modelling resilience

The Cabinet Office presents a framework of four strategic components for achieving resilience, and guides different sector stakeholders towards assessing their need for developing those of the four components necessary for achieving the desired level of resilience (Cabinet Office 2012a). In some cases for example, it may be deemed more cost-effective to accept the cost of the risk and disruption rather than invest in added resilience. According to the framework, resilience is brought about through a combination of:

- **Resistance**, predominantly physical, against the hazard and its direct impact. The limitation of this strategy lies in that the level of resistance is set based on past experience and predictions from historical records. Hence it should not be the only component of a Resilience strategy
- **Reliability,** in the infrastructure's ability to operate adequately across a range of conditions. Again, this strategy is limited to the predicted range of events and might fail to protect against events with impacts beyond this range.
- **Redundancy,** through the availability of spare capacity or backup installations to switch to, in case of disruption to facilities. While the switch may be relatively quick for sectors such as the ICT sector, in sectors like water or transportation there is a period of loss of service until the switch is made.
- **Response and Recovery** plans in place for rapid response and recovery from disruption. While response relates to the ability to minimise the short-term impact on services, recovery requires a more long-term perspective on resilience.

Mapping infrastructure interdependencies is crucial towards developing the above strategies, and a growing body of research is comparing infrastructure systems to Complex Adaptive Systems (CAS), typically used to define biological/ecological systems, in order to map these connections. These are systems where the behaviour of individual components does not have a linear effect on the behaviour of the entire system.

In their work on complex adaptive systems, Holland (Holland 1992) and Gross *et al*. (Gross & Blasius 2008)outlined key characteristics of CAS as those of:

- **Evolution:** as components of a CAS constantly shift to ensure survival they influence the entire system back via their inputs and outputs. This feedback mechanism ensures that

components influence and respond to their environment, thus leading to the evolution of the entire system.

- **Aggregate behaviour:** where the interaction of systems or system components causes **emergent** behaviour that is different to the sum of the behaviours of individual components.

- **Anticipation:** each component within a CAS anticipates changing circumstances in order to respond to them. Although the response of each component may be straightforward, the aggregate response of the entire system can be quite complex to model, even if the anticipated circumstances did not end up occurring.

- **Sub-optimality:** because each component is constantly readjusting to a novel environment brought about by the emergent behaviour of the readjustment, components typically operate far from optimal conditions. A system which settles at an optimum temporarily can become 'dead' if left there for extended periods.

- **Self-governance:** where individual sub-systems are encouraged to self-react, self-organise and self-adapt to their own environment thus constantly shifting the entire system in a new viable position. Variety and diversity are encouraged, as this diversifies its internal competencies, strengths, weaknesses and coping mechanisms and thus increases its resilience to external threat.

- **Self-organisation towards critical behaviour:** the adaptive nature of such networks makes them capable of self-organising towards dynamically critical states on the edge of chaos, undergoing constant re-organisation and innovation, while at the same time still functioning as a whole.

- **Simple rules:** even if behaviour of individual components of CAS is governed by quite straightforward, simple rules, the fact that there is a diversity of rules being acted on at the same time, makes the overall system's behaviour difficult to predict and model.

The above characteristics make modelling of infrastructure as Complex Adaptive Systems very complex. They imply that behaviour of interconnected infrastructure components or sub-systems is historically and context specific, it is dynamic and constantly evolving, it is not

governed by a single rule, it can cascade disturbance through a system and it does not operate at optimal end-points. Pederson *et al*. of the Idaho National Laboratory have conducted a survey of international research in critical infrastructure interdependency modelling with the aim of developing a single source reference for such tools (Pederson *et al*. 2006). These simulations are currently being used by the private sector and government agencies to increase efficiencies, plan developments, enhance redundancy and respond to emergencies. In 2001, the National Infrastructure Simulation and Analysis Centre (NISAC) was established in the US to develop advanced modelling that can identify infrastructure interdependencies and vulnerabilities.

Current barriers to modelling and simulation internationally include the lack of data available in sufficient detail for the construct of detailed models, and challenges in model development and model validation. Interdependency analysis becomes further complicated by the extremely large and disparate cross sector analysis required.

Recommendations

In order to increase resilience of UK infrastructure, the following is recommended.

- The **energy sector** needs to increase physical defence against flooding, increase storage capacity and establish contingency plans to enable rerouting of electricity in case of disruption. To avoid efficiency reduction, future developments should be sited in cooler locations, and awareness-raising should be used to manage energy demand. Smart grid technology should be used to provide reliable energy source diversification, and climate change adaptation measures should be designed into planning towards a low carbon economy, with lessons drawn from energy production in other countries. The sector will require major investment in order to handle intermittency from feeding-in from renewable sources, increased use of heat pumps for household heating, and the increased use of electric vehicles.

- The **transport sector** needs to enforce more frequent inspection, particularly of bridges and clay embankments, and implement an emergency planning regime to deal with passenger health problems during train overheating. Better forecast of storms is needed to ensure that ships and planes arrive at ports and airports safely, else are diverted reliably, and changing wind directions should be incorporated into new airport infrastructure.

- The **water sector** needs to increase the structural stability of existing water storage systems and increase storage as redundancy to ensure security of supply. Sustainable Urban Drainage Systems (SUDS) should also be used to reduce the risk of flooding in densely built areas. The water sector is already taking short-term resilience planning and long term adaptation actions via the preparation of Water Resource Management Plans with a 25 year forecast.

- The **ICT sector** can be said to be already more adaptable and resilient than other sectors to future risks due to the presence of multiple networks, the high rate of innovation and the relatively short anticipated lifetimes of its infrastructure. The modular nature of ICT infrastructure implies that it can more easily absorb innovation in response to disruptions, and that computational load can be shifted from one site to another as needed. Providing re-routing options can increase efficiency and robustness, however when the space

capacity across the entire network is reduced, re-routing might take place through less-than-ideal routes, leading to cascading failure.

- As recommended by the Pitt Review, the UK **government** should create an inter-agency body, the responsibility of which would be to advise the former on matters of resilience, ensuring the government's commitment to a multi-agency, consensual approach. The body would be responsible for policy oversight of national infrastructure in collaboration with industry. It would develop mechanisms for improved knowledge sharing and collaboration between infrastructure sectors and across government agencies and regulators, particularly on issues of resilience, risk and interconnectivity. It would investigate vulnerabilities at critical UK infrastructure interconnections by commissioning research into scenario-planning and modelling, and would enforce the development of safeguards against these. It would investigate barriers created by strategic and legislative frameworks and it would identify and support the development of technologies and skills needed for achieving adequate resilience. The government needs to facilitate greater cooperation and information sharing between companies and sectors and needs to raise awareness and encourage investment in infrastructure adaptation.

- **Regulators** should use their levers to promote adaptation and resilience building against value for money. Instead of encouraging efficiency which reduces resilience, regulations should be revised to reflect future threats and allow more information-sharing and collaboration across the supply chain. Regulators should set probabilistic standards rather than absolute requirements and partial service restoration after an emergency should be allowed, while the remaining is unavailable. Owners should be required to report on resilience annually, establish schemes for monitoring particularly vulnerable sites, should be encouraged to adopt the Business Continuity Management British Standard BS25999. The government should ensure that regulators stimulate and incentivise innovation and that through regulations a business case is being made for resilience, including via the use of service standards.

- **Infrastructure operators** need to realise the benefits of including climate change adaptation and resilience thinking throughout their organisations and asset planning – from physical design to operational procedures and contingency planning. Lost revenues, reputational damage, contractual penalties and the potential for litigation provide strong

drivers for managing risks and building resilience. Operators need to develop a resilience strategy which employs the principles of redundancy, resistance, reliability, response and recovery for protection against disruptions. This strategy needs to have buy-in from other stakeholders including supply chain, customers and operators, it needs to consider Business Continuity Plans as recommended in BS 25999 and needs to be considered at all levels of the organisations. It must be understood that striving for optimisation and efficiency can compromise resilience making infrastructure brittle. Strong at impact, but catastrophic at failure. Instead, operators should aim for elastic infrastructure through sacrificing efficiency for the sake of resilience.

- **Engineers**, via the Sector Skills Councils, should have greater access to training and accreditation on the kind of skills necessary to deliver resilient CNI. This includes training in a systems and life-cycle approach to resilient design, the use of probabilistic methods for dealing with complex risk scenarios, and skills to design multi-purpose, modular, adaptable facilities. These skills and expertise can also be marketed to other countries.

- **Investors** should have greater access to reliable risk and climate change prediction data to inform their decisions. The historically low likelihood of certain high impact events can make their prediction difficult and discourage investment. Support of innovation investment (such as Ofgem's Innovative Funding Initiative) can also lead to improved financing of resilience projects. A business case should be made for resilience investment while new financial mechanisms should to be developed to ensure funds for adaptation are available throughout asset lifetime.

- The development of **Event Standards** could be considered where a level of operations can be assured despite extreme events. This can be achieved by presenting worst case scenarios to operators, against which they can test their resilience and identify gaps for reinforcement. A **standard for resilience** against specific hazards can be introduced, based on the likelihood of the hazard occurring. This would enable the standard to evolve as the likelihood changes.

- **Local businesses and communities**, with the help of their Local Resilience Forums need to understand the risks that could affect them and produce a community risk register. Through business continuity management, risks identified can be assessed and

help improve understanding of critical infrastructure and vulnerabilities. Specific local assumptions can then be developed based on the identified hazards to inform emergency response and investment decisions.

- Infrastructure interdependency **modelling and simulation** will be key in identifying critical risks and vulnerabilities to UK infrastructure systems. Research should be commissioned which has the expertise, financial resources and multi-sectoral data in sufficient detail such as to develop robust, reliable models. This will be rewarded with the identification of concrete areas in need of investment both for reducing vulnerabilities and for having a competitive advantage over emerging opportunities.

References

Buldyrev, S.V. *et al*., 2010. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291), pp.1025–8. Available at: http://www.ncbi.nlm.nih.gov/pubmed/20393559 [Accessed October 27, 2012].

Cabinet Office, 2012a. *A Summary of the 2012 Sector Resilience Plans*,

Cabinet Office, 2011. Keeping the Country Running: Natural Hazards and Infrastructure.

Cabinet Office, 2012b. *National Risk Register of Civil Emergencies*,

Chang, S.E., 2009. Infrastructure Resilience to Disasters. In *2009 Frontiers of Engineering Symposium*. pp. 1–4. Available at: http://www.nae.edu/File.aspx?id=15629.

Council for Science and Technology, 2009. *A National Infrastructure for the 21st Century*,

DEFRA, 2011. *Climate Resilient Infrastructure: Preparing for a Changing Climate*,

Department of Homeland Security, 2012. Critical Infrastructure.

Fildes, J., 2011. Stuxnet virus targets and spread revealed. *BBC News*. Available at: http://www.bbc.co.uk/news/technology-12465688 [Accessed June 11, 2012].

Frontier Economics, 2012. *Systemic Risks and Opportunities in UK infrastructure*,

Gross, T. & Blasius, B., 2008. Adaptive coevolutionary networks: a review. *Journal of the Royal Society, Interface / the Royal Society*, 5(20), pp.259–71. Available at: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2405905&tool=pmcentrez&rendertype=abstract [Accessed November 4, 2012].

Holland, J.J., 1992. Complex Adaptive Systems. *MIT Press*.

Natural Resources Canada, 2006. *Final Report on the Implementation of the Task Force Recommendations*, Available at: http://www.nrcan.gc.ca/sites/www.nrcan.gc.ca.energy/files/pdf/eneene/pdf/outpan-eng.pdf.

Pederson, P. *et al*., 2006. *Critical Infrastructure Interdependency Modeling : A Survey of U.S. and International Research*,

Pitt, M., 2007. Learning lessons from the 2007 floods.

Rinaldi, B.S.M., Peerenboom, J.P. & Kelly, T.K., 2001. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, pp.11–25.

US Department of Energy, 2011. *Critical Materials Strategy*,

Walker, B. *et al*., 2004. Resilience , Adaptability and Transformability in Social – ecological Systems. *Ecology And Society*, 9(2). Available at: http://www.ecologyandsociety.org/vol9/iss2/art5/.

World Economic Forum, 2010. *Global Risks 2010: A Global Risk Network Report*,

Foresight
1 Victoria Street
London SW1H 0ET
www.foresight.gov.uk
URN 12/1310