Socio-Technical Approaches to Risk Assessment in National Critical Infrastructures

Deregulation has created new market pressures for innovation across many national infrastructures. This, in turn, creates complex interdependencies. For example, in previous years both the US and European energy markets relied upon vertical integration. The same companies that generated the power were also, typically, responsible for its transmission to consumers. This market structure creates barriers to new generators who cannot access the transmission systems, which are owned and operated by their existing rivals. In consequence, successive administrations have introduced vertical separation of transmission and generation in order to increase competition and innovation in energy production. However, without complex regulatory mechanisms it can be hard to ensure that the underlying physical infrastructure can reliably support the transmission of energy from these new producers to their potential consumers. The stress created by large transfers of energy across aging infrastructures and unprecedented distances has been a cause of pan-regional blackouts across areas of Europe and North America (Johnson, 2008).

It is important to stress that many of these changes are not isolated within the energy industries. 'Just in time' production techniques have been extended to logistics; automated ordering and dispatch systems control the delivery of everything from food through to drinking water and even the aircraft that operate the daily schedules of most aviation companies. Small changes can have extraordinary and unpredictable consequences. For example, a delay of only a few minutes to an aircraft departure can leave airlines struggling for many hours to catch up with their schedule. Similarly, passengers at the UK's new Heathrow Terminal 5 experienced huge delays and many hundreds never received their luggage because baggage handling teams were not correctly rostered to those areas where they were most needed.

In the aftermath of 9/11, much of the work on national critical infrastructures has focussed on the vulnerability of systems to coordinated terrorist attack. This is certainly reflected in several of the papers that were published in a previous special edition of this journal on national critical infrastructures (Volume 92, Number 9, September 2007). However, the balance is perhaps changing. This special edition contains a number of articles that formed part of a follow-up workshop on socio-technical issues in risk assessment in infrastructure systems. For instance, Chozos presents a study of the human and organisational issues that affect the reliability of care within a national healthcare system. In order to understand the likelihood and consequences of adverse events within such 'infrastructure' applications it is important to ensure that we detect previous failures. Without an accurate picture of existing provision, it is difficult to envisage the risks and associated hazards that might arise from any future system of healthcare. However, as Chozos shows, we know remarkably little about those procedures and mechanisms that help to ensure incident reports are acted upon. In many cases, the concerns of nurses, junior doctors and patients, are not treated with sufficient concern. Increases in morbidity can be explained in terms of the underlying health of the patients or a host of other factors that are not directly associated with the quality of healthcare provided. It seems clear from his analysis that such problems would give rise to considerable concern if they occurred in almost any other form of national infrastructure. As with the other papers in this collection, the paper stresses the social and organisational barriers that can make it difficult to assess the risks that undermine service provision across a range of critical industries.

Sommerville, Storer and Lock focus on a more conventional area of infrastructure protection. Their contribution considers contingency planning for potential floods. This paper is of particular importance given the recent severe flooding events to strike the UK, in Cumbria in 2005 and from Yorkshire through to Gloucestershire in 2007, and many areas of the United States, especially Oregon and Washington in December 2007 and the Midwest during Spring and Summer 2008. They point out that accurate risk assessments during contingency planning depend upon the identification of relevant stakeholders. Equally the mitigation of any adverse consequences also depends upon the accurate identification of those agencies that are primarily responsible for different aspects of any emergency response. Unless there is clarity over responsibility then it is likely that any interventions will be complicated by a host of additional socio-technical problems including communications barriers and the consequent waste of precious resources. Sommerville, Storer and Lock identify the diverse range of stakeholders that must be considered by emergency agencies as they struggle to restore critical infrastructures. Their work forms a useful contrast with Chozos' work, mentioned in the previous paragraph. His work on healthcare looks at the organisational response to single adverse events in 'routine healthcare' while the work of Sommerville, Storer and Lock considers the reaction of several complex agencies in extraordinary contingencies.

Smith and Fischbacher continue organisational focus introduced by Sommerville et al; both papers deal with the complexities of inter-organisational communication and coordination in critical infrastructures. Whereas Somerville, Storer and Lock look at the response to a civil contingency, Smith and Fischbacher focus more narrowly on the role that human networks between organisations can play in the incubation and escalation of crises. They acknowledge the diverse hazards and threats that can lead to risks in socio-technical systems. However, they make a strong and compelling argument that there are certain classes of inter-organisational networks that affect the ways in which those risks might be realised and compounded, for example by ignoring or acting upon previous warnings about potential failures. There are, therefore, strong links with the work of Chozos' in his investigation of the factors that prevent prompt action in response to concerns over healthcare incidents. Smith and Fischbacher argue that the ways in which information flows within and between organisations has a profound impact upon the incubation of risks in national infrastructures where, as have seen, there are increasing moved to separate supply from generation or infrastructure maintenance from service provision. In addition to the organisational networks that structure communication between different companies, this paper also identifies the influence of social and professional networks in shaping both the planning for and response to adverse events. In other words, the 'accepted wisdom' about the criticality of particular risks can be determined by an individual's involvement in social, organisational and professional networks. This is increasingly important because we often make incorrect assumptions about the resilience of interconnections with other critical infrastructures. It is hard for many engineers and managers to assess the reliability of the systems that they operate and maintain because they cannot characterise the reliability of the computer networks or power distribution systems that they depend upon. Engineers and managers may lack this information because they do not have access to the organisational, social and professional networks where there potential infrastructure failures are considered. For instance, it can be difficult for power transmission companies to assess the ability of other areas of a network to support particular levels of loading because this can be considered business critical information for the transmission company.

Anderson and Felici expand on some aspects of Smith and Fischbacher's work when they consider the different ways in which communities are formed around particular technologies. In order for someone to understand the risks associated with those technologies it is first necessary to interact with the technical groups that have been formed to support the application of these systems. Anderson and Felici go on to explain that the consequences of the risks created by these technologies are seldom restricted to these technical groups. However, the public who are most directly affected by an accident may depend upon these technical associations to provide an explanation of the reasons why a system failed. They illustrate aspects of this argument with examples drawn from the growth of safety-critical computer systems where systems engineers both promote the development of these applications and lead the analysis of previous failures. This can lead to potential problems when the 'communities of practice' that form around critical technologies have a primary interest in microscopic technical issues rather than the macroscopic social and environmental concerns that may be most pressing for the general public who are 'at risk' from the application of these technologies. In terms of critical infrastructures, Anderson and Felici identify what they term 'boundary objects' that create an interface between several of these groups. Hence the users of electricity have an interface with those who transfer it and they, in turn, have an interface with those who generate the electricity in the first place. It, therefore, becomes critical to identify ways in which these different groups can communicate the risks and dependencies that exist between these interfaces. Too often failures occur because of subtle differences in the language and terms used by these different groups of stakeholders especially given the dynamic nature of many critical infrastructures. For instance, several recent blackouts have stemmed from confusion over the extent of the restrictions that may be placed on transmission during particular times of the year – when for instance high power lines may come into contact with increased vegetation.

The final paper in this collection returns to themes introduced by Chozos in the first contribution. Rather than look at the external threats created by, for instance, terrorist attacks, Johnson, Kirwan and Licu look at the hazards that are created by the everyday operation of national transportation systems. Their work focuses on the impact of degraded modes of operation in Air Traffic Management. A degraded mode occurs when operators struggle to maintain levels of service provision even when technical failures have compromised elements of their underlying infrastructure. This has important consequences; 'degraded modes' have been identified as contributory factors behind the Linate runway incursion and the Uberlingen mid-air collision that remain the worst European accidents associated with Air Traffic Management. This paper looks at the different approaches adopted by European service providers in responding to 'everyday' failures. Rather than look at the engineering and process issues, the focus is on the interaction between 'safety culture' and degraded modes of operation. In other words, the paper is motivated by a desire to understand why many operational teams will continue to work even when they have lost many of the systems that they would otherwise rely on. This is particularly significant given that the other papers in this collection have shown how little we know about the interdependencies that exist between these infrastructure applications. In the Uberlingen accident mentioned above, it was difficult for the Air Traffic Control Officer to identify the many different ways in which maintenance work had affected the computer networks that supported his operating environment.

To sum up, this collection provides a socio-technical perspective on the risks associated with national critical infrastructures. The intention is not to promote a purely sociological view where the focus is mostly on the implications of infrastructure failure on society. Instead, we would adopt

an engineering and management perspective that seeks to understand basic issues such as ‘why don’t we act on the reports of previous failures until it is too late?’ or ‘why do we keep operating systems even when they’re broke?’ or ‘why can’t we decide on who is responsible for fixing this infrastructure when things go badly wrong?’.

Chris Johnson, Glasgow, Scotland, 30th July 2008.

http://www.dcs.gla.ac.uk/~johnson

Reference

C.W. Johnson, Understanding Failures in International Infrastructures: A Comparison of Major Blackouts in North America and Europe. To appear in the Proceedings of the 26th International Conference on Systems Safety, Vancouver, Canada 2008.