Computational Support for Identifying Safety and Security Related Dependencies between National Critical Infrastructures

Chris. W. Johnson and Rhys Williams

Department of Computing Science, University of Glasgow, Scotland, UK, Johnson@dcs.gla.ac.uk

Keywords: Critical national infrastructures, counter-terrorism, contingency planning.

Abstract

Previous terrorist attacks, system failures and natural disasters have revealed the problems that many States face in preparing for national civil contingencies. The diversity of critical infrastructures and the interconnections between different systems makes it difficult for planners to 'think of everything'. For example, the loss of power distribution networks can disrupt rail and road transportation systems. Knock-on effects can also be felt across telecommunications infrastructures as the uninterruptible power supplies (UPS') that protect Internet routers and mobile phone base stations fail over time. Domestic water supplies are affected when pumping and treatment centres lose power. These interconnections make it hard to anticipate the many different safety-related systems that might be affected by particular contingencies. This paper introduces a Geographic Information System that is intended to help government agencies plan for the knock-on effects that propagate between major infrastructures. The intention is to provide a flexible system, which can easily be configured and updated. This is important given that technical innovation and routine maintenance continually introduce changes across national infrastructures.

1. Introduction

In the aftermath of terrorist attacks in New York, Madrid and London, there is growing awareness of the vulnerability of many states to terrorist attack. Similarly, natural disasters such as Hurricane Katrina, Tropical Storm Alison and the floods that affected many different areas of the UK during 2007 have revealed the difficulty that many nations face in coordinating their preparations for civil contingencies. One of the most common criticisms in the aftermath of these events is the 'lack of joined up thinking' by government agencies. The Federal joint task force into the 2003 Blackout across the North Eastern United States and parts of Canada identified 'surprising' vulnerabilities across different infrastructures once a domino effect began to propagate failure across and between the national grids [1]. The 9/11 Commission repeatedly refer to the 'lack of imagination' in planning for terrorist attacks [2]. A Federal 'lessons learned' report into Hurricane Katrina refers to the fragmentation of planning and the lack of coordination across government agencies in preparing for the response to a contingency that had been anticipated [3].

One reason why we have been so unprepared for previous contingencies is the very diversity of national critical infrastructures. For example, the US National Strategy for the Physical Protection of Critical Infrastructures and Key Assets focuses on: agriculture and food; water; public health; emergency services; defence industrial base; telecommunications; energy; transportation; banking and finance; chemicals and hazardous materials; postal and shipping [4]. The UK Centre for the Protection of National Critical Infrastructures (CPNI) identifies nine sectors which deliver essential services: energy, food, water, transport, telecommunications, government & public services, emergency services, health and finance. It is a difficult enough task to understand how any one of these different infrastructures might be affected by a terrorist attack, natural disaster or technical failure without considering the knock-on effects that complicate our response to civil contingencies [5].

2. Scoping the Problem

There are very few tools that government agencies might use to identify the dependencies that extend between national critical infrastructures. This is not surprising given the challenges involved in developing such an application. In particular, it can be difficult to identify the range of adverse events that might trigger the failure of energy systems, food, water, transport, telecommunications etc. Political considerations, public anxiety and the influence of the media all add to the difficulty that commercial and public agencies face in identifying potential hazards and threats to critical infrastructures. Many potential scenarios have an extremely low likelihood. These cannot, however, be ignored because the consequences of these events can be enormous. The UK National Risk Register presents an 'assessment of the likelihood and potential impact of a range of different risks that may directly affect the UK' as part of the National Security Strategy [6]. The Register provides a snap-shot of the most significant emergencies that have been identified over a five-year time scale. These are classified as either accidents; natural events, collectively known as hazards, or malicious attacks, known as threats. Figure 1 summarises the range of risks considered within the 2008 UK national register.

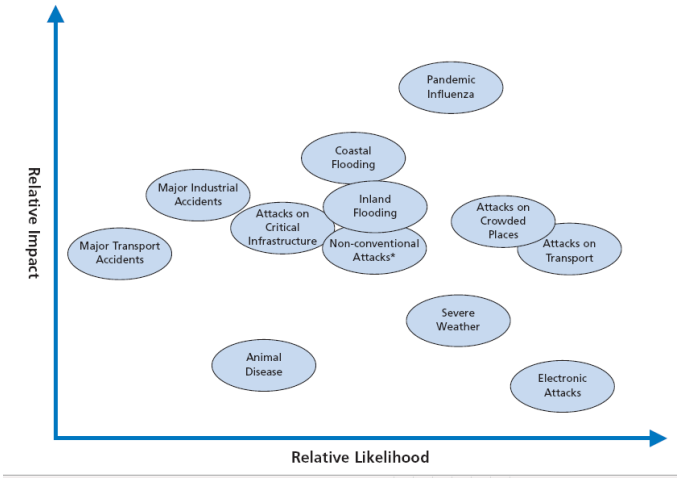

Figure 1: High Consequence Risks Facing the UK [6]

3. Examples of Civil Contingencies

An important aim behind the work described in this paper is to provide computational tools that support the high-level and subjective assessments of 'relative impact' for the infrastructure risks identified in Figure 1. In order to do this, it is critical that as much information as possible is obtained from previous adverse events. Many of the risks shown in Figure 1 have not affected the UK. We must, therefore, build on experience gained in other countries. This creates problems; skeptics often argue that lessons learned in one state cannot be applied in the context of other national infrastructures. These objections are increasingly difficult to sustain given that common themes have characterized diverse contingencies in many different countries. In particular, the response to adverse events is often hindered by a lack of 'joined up' thinking both in terms of the impact that contingencies can have upon national infrastructures and the consequences that knock-on effects will have upon subsequent intervention.

A number of previous national civil contingencies illustrate the ways in which failures can propagate across infrastructures to threaten public safety. A blackout in 2003 affected areas of France, Switzerland and almost all of Italy. This left 30,000 people trapped on trains. The scale of the knock-on effects created by the blackout forced emergency services to develop a range of ad hoc solutions as they called upon the support of many more agencies than were originally intended within the existing contingency plans. Other knock-on effects were arguably less dramatic in terms of their impact on public safety. However, they had considerable consequences in terms of the distress caused to the individuals concerned. For example, Pironi, Spinucci and Paganelli describe how the blackout affected patients that relied on home parenteral nutrition systems [7]. These individuals used electronic pumps for the overnight infusion of nutritional solutions. The loss of power disrupted their treatment. Different devices responded in different ways as some began to generate alarms while others reverted to battery power. Patients responded in different ways as they became worried about whether or not their systems had sufficient power to complete their treatment for that night. The blackout lasted several days across many areas of Italy. This created further problems as stores of parenteral solution had to be stored in freezers. Other patients were placed at risk when the loss of power began to affect water treatment centres. It became difficult to guarantee that there was no microbiological or toxic contamination in the water supplies for dialysis patients.

The inter-dependencies between power distribution and healthcare are strongly affected by technical, social and political factors. The UK's 'care in the community' initiative has encouraged many patients to take responsibility for treatment in their own homes. This moves them away from the UPS' that provide backup power to hospitals and other healthcare centres. While this reduces costs and can improve the quality of life for many individuals, it also exposes some patients to the risks of knock-on effects when power supplies are interrupted to domestic properties.

There are many further examples of the knock-on effects that complicate the response to civil contingencies. The decision to halt Underground services following the July bombings in London pushed thousands of commuters onto the remaining bus services that might themselves have been secondary targets. Official reports into the bombing also describe problems created by the failure to establish reception centres for victims and their families/friends in the hours after the blasts. People did not know where to look and, in consequence, the Casualty Bureau phone line received many more calls in the first 24 hours than in any previous emergency. At its peak this rose to 43,000 attempted calls in an hour. The system was overwhelmed. This aspect of the response to a civil contingency is instructive because it illustrates the way in which problems in establishing physical centres to provide support in the aftermath of the bombings created knock-on effects for the communications and information infrastructure [8].

The number of fatalities directly attributable to a lack of planning in the Federal response to Hurricane Katrina remains a subject of considerable controversy. It is clear, however, that the scale and timing of the evacuations created immense strains for the host communities. There were also considerable, unexpected problems in coordinating the inter-agency response when so many diverse aspects of the transport, power and telecommunications infrastructures were affected by flooding and high winds. The Presedential report into 'lessons learned' summarised the problems created by knock-on effects between the communications and power infrastructures; "the storm debilitated 911 emergency call centers, disrupting local emergency services. Nearly three million customers lost telephone service. Broadcast communications, including 50 percent of area radio stations and 44 percent of area television stations, similarly were affected. More than 50,000 utility poles were toppled in Mississippi alone,

meaning that even if telephone call centers and electricity generation capabilities were functioning, the connections to the customers were broken...Although Federal, State, and local agencies had communications plans and assets in place, these plans and assets were neither sufficient nor adequately integrated to respond effectively to the disaster" [3].

4. Difficulties in Mapping National Infrastructures

A number of difficulties must be addressed before any tool can help to identify the knock-on effects that can arise between infrastructures that during civil contingencies.

What is a Critical Infrastructure? Previous sections have enumerated the critical systems identified by the US National Strategy for the Physical Protection of Critical Infrastructures and Key Assets and the UK CPNI. We have also summarised the most significant risks to these infrastructures identified as part of the UK National Security Strategy. However, national and regional agencies must look beyond this high-level guidance in order to develop the more detailed policies and procedures that are required during future contingencies. For example, the CPNI list of critical infrastructures refers to 'transportation'. It is unclear whether or not a contingency planning tool should therefore consider the impact of a prolonged loss of power on our national Air Traffic Management centres or on railway signalling systems, on the traffic lights that coordinate urban traffic movements or on the cameras that help police monitor the motorway system. In the past it has been argued that these individual systems cannot be regarded as 'critical' because alternate forms of transport would be available. As we have seen, however, the interdependencies between critical systems make it dangerous to assume that a single adverse event could not undermine several different modes of transport at the same time. Pandemics and other forms of disease are an obvious example. This more integrated view of contingency planning makes it increasingly difficult to exclude systems from the national critical infrastructure.

Legacy Systems, Maintenance and Replacement Programmes: Many European states rely on infrastructures that were first built more than a century ago. The continued operation of these systems is a testament to the engineers who created them. However, the three dimensional mapping techniques and record keeping processes that were used during the development of these systems was inconsistent. In consequence, we do not know the precise routes that are used by many of the water and power networks that are integrated with more modern infrastructures. Any system to assess the inter-dependencies between infrastructures must therefore deal with significant uncertainty about the topography of the underlying networks.

Further challenges stem from the rolling programmes that have been created in many countries to replace aging infrastructures. These upgraded networks often follow very different routes from legacy systems. Their introduction can create new interdependencies, where for example advanced sensing technologies are deployed to monitor energy transfers in real time. The operation of the power distribution infrastructure, therefore, relies on both the connectivity of the network itself but also on the digital data exchange systems that are used to control loads across increasingly complex architectures.

The impact of these replacement programmes can be compounded by the changes that must be made to infrastructures in response to demographics. Population movements, away from many urban centres have triggered the redeployment of fire and rescue services. These changes can also lead to the development of new power supplies, water and transportation infrastructures etc. It can be difficult to ensure that modelling tools for infrastructure resilience are updated to keep pace with the changes in the associated infrastructures. Tools that assess infrastructure resilience must, therefore, be regularly updated as replacement programmes, population movements, changes in industrial processes all trigger significant changes to underlying infrastructures.

Vertical Separation of Infrastructure Markets: Traditionally, state run monopolies were established to focus the investment necessary to create and maintain power, water and transportation networks. These were vertically integrated so that the same organisations provided the service and controlled the infrastructures. For instance, electricity generators also owned the distribution system. Similarly, national rail organisations operated the trains and helped to maintain the tracks and signalling systems. Initiatives such as the European Commission's Electricity Directive 96/92 sought to reduce the state's role in service provision. The aim was to reduce costs for customers by opening markets to competition from companies in other member states. In order to do this, the operation and maintenance of underlying infrastructures had to be separated from service provision. If this vertical separation had not been implemented then new market entrants that would have been forced to use their competitors' infrastructure. The consequences of this vertical separation of service providers from infrastructure operators cannot be underestimated. One of the causes behind both the US and European blackouts of 2003 was the difficulty that infrastructure providers faced in assessing the demands that service providers would place on their networks, for example as they sought to transfer increasing amounts of energy from low-cost generators to remote sources of demand [5]. Not only has the vertical separation of infrastructure markets led the failure of service provision across international borders, it also frustrates attempts to models the knock-on effects of infrastructure failures. The events of 2003 illustrate the difficulties that energy providers face in modelling the dependencies within their own industry without considering the interactions with other infrastructures.

Innovation and change: Further problems frustrate attempts to model the knock-on effects of failures in national critical

infrastructures. Technical innovation affects the composition and structure of complex systems. The rapid deployment of fibre optic and mobile communications systems, the gradual introduction of Internet based systems in SCADA applications, the development of local and renewable power generation systems are all changing the interdependencies between infrastructures. Unfortunately, we know very little indeed about how these novel systems will perform under many of the scenarios summarised in the UK National Risks Register.

It can be difficult to determine the impact that particular contingencies might have upon the exchange of digital data. This has motivated many safety-related industries to develop dedicated networks that are believed to offer higher levels of resilience than the public Internet. Hurricane Katrina and the UK floods of 2006 have shown that such optimism is not always justified. In contrast, increasing numbers of commercial and government organisations are using Internet based communications for the exchange of critical information. A number of studies have been conducted into the impact of the 2003 US-Canada blackout on Internet traffic. Abnormal Border Gateway Protocol (BGP) events indicate that 3,175 networks lost connectivity. Most of these were in the New York City area [9]. Although we have forensic techniques that can help identify patterns of failure across the Internet under contingencies, we are a long way from being able to conduct more predictive forms of analysis at a national or regional level. In particular, there are no agreed means of modelling the effects of any future power system failures on the UK computational infrastructure. This, in turn, makes it impossible to anticipate the secondary impact of the loss of Internet connectivity on the increasing numbers of critical systems that rely upon these networks for the exchange of operational information.

Technical innovation can also increase resilience. For example, the Pitt review into the UK floods of 2007 describes how telecommunications companies were surprised by how well some of their networks stood up to water inundation. This was due to traditional copper wire cabling gradually being replaced by new forms of fibre optic interconnection. Even so, the report identifies the risks associated with dependencies that extend beyond individual national infrastructures; “flooding has the capability to disable networks when coupled with power failure” [10].

5. The Infrastructure Dependencies GIS

Figure 2 provides a snap shot of the interface to a Geographical Information System that exploits Bayesian techniques to generate failure scenarios across national critical infrastructures. The decision to focus on Scotland rather than the United Kingdom is justified by the need to gather a range of sensitive data during the preliminary stages of the project. Given the lack of existing tools, the Infrastructure Dependencies GIS (ID-GIS) represents an initial prototype. As can be seen, however, the user can add or remove critical nodes and links between different infrastructures including the domestic water supply, major gas interconnections, and national electricity distribution etc.

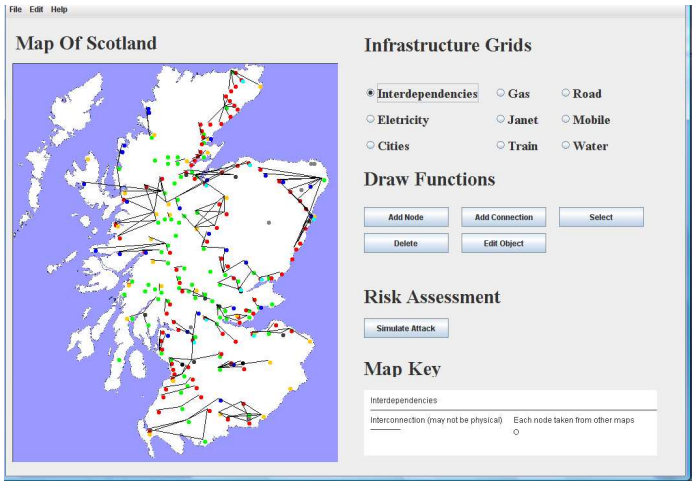

Figure 2: Infrastructure Dependencies GIS (ID-GIS)

The ability to map national critical infrastructures onto a common GIS provides relatively few additional insights for contingency planning. In particular, it fails to address many of the barriers that were identified for predictive modelling of knock-on effects that were identified in Section 4. Geographical proximity fails to account for the diverse logical and operational dependencies that increasingly connect different systems. Fortunately, a range of algorithms have recently been developed in the US and Canada to help planners predict the value or importance of particular elements in national critical infrastructures [11, 12]. Some of these algorithms consider inter-infrastructure dependencies; however, most previous work has focused on urban districts rather than national infrastructures.

As mentioned, the lack of vertical integration, the problems of mapping legacy infrastructures, the introduction of new technologies all combine to undermine attempts to trace the detailed ways in which faults propagate between critical national infrastructures. It will take several years before we can identify the precise impact that the loss of key components will have upon the systems that depend upon them. In particular, we cannot easily identify the knock-on effects that would arise if we were to lose significant sections of our digital communications and power distribution networks. Fortunately, Bayesian statistics provide an alternate to the detailed causal modelling of infrastructure interdependencies. Expert judgement can be used to assess the dependent probability of a system failing given that problems have been observed in another infrastructure. Where possible, these estimates can steadily be refined with more accurate probability distributions based on partial causal models or from data obtained during previous contingencies, such as those cited in Section 3.

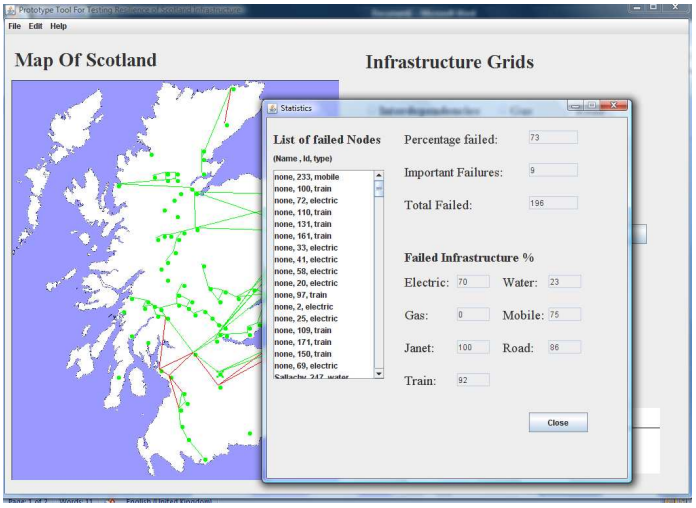

Figure 3: Knock-on Effects of Single Node Failures

Figure 3 shows how the user of the ID-GIS can select particular nodes across the electricity, transport and digital communications network to assess what might happen if they were to fail. Knock-on effects propagate between infrastructures using Bayesian probability distributions in the manner described above. The intention is not to identify the many detailed causal mechanisms that for example cause particular Internet routers to fail during a blackout. However, this information can be integrated into the modelling if it is available. In contrast, the intention is to identify subjective probability distributions that can help drive 'what if' scenarios. For instance, during initial evaluations we have used the ID-GIS to investigate the improvement in **systems resilience** that can be achieved by adding sub-networks in the power distribution infrastructure. The central contribution of our work is that increased resilience is not simply calculated in terms of the power systems themselves but in terms of the various other national infrastructures that also depend upon the electricity supply.

6. Conclusions

Previous terrorist attacks, infrastructure failures and natural disasters have revealed the problems that many States face in preparing for national civil contingencies. The diversity of critical infrastructures makes it difficult for planners to 'think of everything'. One aspect of this is that it can be hard to identify the interconnections that exist between different safety-related systems. Some of these dependencies are created by political initiatives. For example, the impact of electricity blackouts on healthcare system has increased as more patients are cared for in their own homes. This often leaves them unprotected by the backup UPS' that support hospital-based treatment. Technical innovations have also created interdependencies. In particular, the integration of Internet communications in a host of critical systems has created vulnerabilities that are often difficult to anticipate before a failure occurs. Very little is known at present about the precise impact of power failures on the routers whose interactions help to regulate traffic flow across this communications infrastructure.

This paper has briefly introduced a Geographic Information System that is intended to help government agencies plan for the knock-on effects that propagate between major infrastructures. We do not know enough about the precise nature of these interactions to develop specific and detailed causal models. The blackouts in the US and Canada and across Europe during 2003, illustrate how little we know even about the failure mechanisms associated with individual infrastructures. In consequence, we have extended a Bayesian approach that integrates expert judgements about dependent probabilities for the failure of one component given that problems have been observed in another infrastructure. This approach also allows for the integration of specific probability distributions where more accurate, causal information is available. However, it is important to stress that this is only an interim solution. We would like to associate confidence levels with the scenarios that are derived from the simulations. In other words, we can direct the system shown in Figures 2 and 3 to simulate the knock-on effects that might be experienced when one or more nodes are removed from different national infrastructures. Given that expert judgements are involved in the underlying calculations, we would also like to estimate the confidence that different experts place in the scenarios that are produced when the system identifies knock-on failures.

A number of other areas remain to be addressed before the ID-GIS and similar tools can provide adequate support for national contingency planning. For example, the provision of Uninterruptible Power Supplies (UPSs) helps to delay the knock-on effects of some infrastructure failures. Battery power can sustain mobile telecommunications base stations for several hours. Hospitals and other key assets have independent generating capacity, although a key lesson of Hurricane Katrina is that these cannot be relied upon in all potential scenarios. At present, the tools described in this paper do not account for the mitigating effects of these systems in delaying the impact of infrastructure problems. Further work could consider these temporal properties through the introduction of more complex stochastic approaches based on Markov chains. However, our initial experience suggests that end users may not understand the underlying mechanisms of the mathematical models.

Further work is needed to improve the techniques that are used to represent infrastructure dependencies. At present probabilities are associated with the individual nodes in each infrastructure. Problems arise when attempting to derive distributions for the failure of multiple network components across complex topologies. Given the redundant and interconnected architectures used for power distribution, the likelihood that a water treatment plant will be affected by the failure of a particular line depends on

both the number of other failures that affect the electricity distribution network and the topology of that network.

A final limitation is that we have an impoverished model of the failure modes that can affect critical systems. We consider only the probability that the failure of one node would lead to the failure of another between different infrastructures. This is unrealistic; many services may not be halted entirely but can continue to function at a reduced rate. For example, traffic will continue to flow through a road system even if the power to the traffic signalling infrastructure has been lost. These caveats should make it clear that our work is only a first step towards the development of more integrated tools for the protection of national critical infrastructures.

Acknowledgement

The original idea for the systems described in this paper came from Mike Corcoran, DSTL. All errors of omission and commission are, however, entirely those of the co-authors.

References

[1] U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, Washington, April 2004. Available on https://reports.energy.gov/BlackoutFinal-Web.pdf, last accessed March 2008.

[2] US National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report, Washington DC, 2004. Available from: http://www.gpoaccess.gov/911/index.html, last accessed March 2008.

[3] Department of Homeland Security, The Federal Response to Hurricane Katrina, Lessons Learned, Washington DC, February 2006. Available on http://www.whitehouse.gov/reports/katrina-lessons-learned.pdf, last accessed March 2008.

[4] National Infrastructure Advisory Council (NIAC) , U.S. Department of Homeland Security, US National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, Washington DC, February 2003. Available on: http://www.whitehouse.gov/pcipb/physical.html last accessed March 2008.

[5] C.W. Johnson, Public Policy and the Failure of National Infrastructures, International Journal of Emergency Management, (1)4:18-32, 2007.

[6] UK Cabinet Office, National Risks Register, Available on: http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx, last accessed August 2008.

[7] L. Pironi, G. Spinucci and F. Paganelli, Effects of the September 28 2003 blackout in Italy in patients on home parenteral nutrition (HPN), Clinical Nutrition, (23)1:133, February 2004.

[8] UK Home Office, Addressing Lessons From the Emergency Response To The 7 July 2005 London Bombings: What we learned and what we are doing about it, 22 September 2006. Available on: http://security.homeoffice.gov.uk/news-publications/publication-search/general/lessons-learned, last accessed August 2008.

[9] J. Li, D. Dou, Z. Wu, S. Kim and V. Agarwal, An Internet Routing Forensics Framework for Discovering Rules of Abnormal BGP Events**,** ACM SIGCOMM Computer Communication Review, (35)5:55-66, 2005.

[10] Pitt Review learning Lessons from the 2007 Floods (Interim report), Cabinet Office, London, UK, December 2007.

[11] G.E. Apostolakis and D.M. Lemon, A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities due to Terrorism, Risk Analysis, 25:361-376, 2005.

[12] J. Zhuang and V.M. Bier, Balancing Terrorism and Natural Disasters—Defensive Strategy with Endogenous Attacker Effort, Operations Research 55(5): 976-991, 2007.