Public Management Review, 2013
Vol. 15, No. 3, 330–343, http://dx.doi.org/10.1080/14719037.2013.769851

Abstract

This article considers the challenges for hospitals in the United Kingdom that arise from the threats of mass-casualty terrorism. Whilst much has been written about the role of health care as a rescuer in terrorist attacks and other mass-casualty crises, little has been written about health care as a victim within a mass-emergency setting. Yet, health care is a key component of any nation's contingency planning and an erosion of its capabilities would have a significant impact on the generation of a wider crisis following a mass-casualty event. This article seeks to highlight the nature of the challenges facing elements of UK health care, with a focus on hospitals both as essential contingency responders under the United Kingdom's civil contingencies legislation and as potential victims of terrorism. It seeks to explore the potential gaps that exist between the task demands facing hospitals and the vulnerabilities that exist within them.

Key words

Organizational crisis, vulnerability, hospitals, terrorism, insider threats

THE VULNERABILITY OF PUBLIC SPACES

Challenges for UK hospitals under the 'new' terrorist threat

Denis Fischbacher-Smith
and Moira Fischbacher-Smith

Denis Fischbacher-Smith
Adam Smith Business School
University of Glasgow
Glasgow
UK
E-mail: denis.fischbacher-smith@glasgow.ac.uk

Moira Fischbacher-Smith
Adam Smith Business School
University of Glasgow
Glasgow
UK
E-mail: moira.fischbacher-smith@glasgow.ac.uk

Routledge
Taylor & Francis Group

INTRODUCTION

A patient walks into a hospital dragging a wheeled suitcase. To all intents and purposes, the individual is coming into the hospital for a procedure and seems to be expecting an overnight stay at the very least. No one checks the suitcase. This patient, however, seeks out the nuclear medicine department intending to detonate 20 kg of home-made explosive, called 'Mother of Satan', which is in the suitcase. He hopes not to die in the initial blast so he can roam the hospital attacking people with the 9-mm firearm that he has hidden on his person. The aim of this attack is to cause mass panic and casualties and to render the hospital impotent in dealing with the aftermath of simultaneous attacks planned across the city. As the hospital is designated as a major trauma centre within the city's civil emergencies plan, this attack will prevent it from receiving the casualties from the other attacks. As such, the hospital attack is part of a wider strategy to destabilize the city and its infrastructure.

The opening scenario to this article is based on observations made by the authors within UK hospitals. Whilst such a scenario may seem fanciful, it is far from impossible. The hospital system (like many public services) is permeable and open. Its security-based defences would appear to be underpinned by a key assumption, which is that no one would actively seek to cause harm within a hospital. This view, however, is based on framing the problem through a Western-centric moral lens that would condemn indiscriminate killing of innocents, especially of those who are already ill.

A similar view prevailed within education prior to the fatal attacks at Dunblane (UK), Columbine (USA) and Beslan (Russian Federation), but those attacks changed the dominant mindset around the vulnerabilities of schools to external mass-casualty threats involving firearms. The Oklahoma City bombing, the Oslo shootings and even the Tokyo subway gas attacks all illustrated the vulnerability of public services to terrorism. These cases also illustrate the risks from domestic, often described as home-grown terrorists (Durham, 1996; Mulinari and Neergaard, 2012; Olson, 1999). The shocks caused by such extreme events have been seen to generate shifts in the views held by policy-makers regarding potential risks of this nature (Field, 2009; Savitch, 2003; Vidino, 2007), even in the most consensus-seeking societies (Reader, 2001). The challenge for public management is how to change that dominant paradigm before a terrorist attack so that effective defences can be put in place to prevent it.

A related challenge stems from a growing recognition that cities are the focal point of terrorist attacks in what has been likened to an 'urban battlespace' (Graham, 2009; Sorkin, 2008). Following on from the attacks on Mumbai in 2008 (Tankel, 2011), there has been considerable attention paid to the vulnerability of cities, especially to roving attacks by terrorists (Bishop and Roy, 2009; Fischbacher-Smith *et al.*, 2010; Sassen, 2010). Much of the response to the range of terrorist threats has been the increase of surveillance within cities, although concerns have been raised as to whether such an approach will prove successful in preventing attacks (Haggerty and Gazso, 2005).

What is also clear from Mumbai attack is that the very technologies that underpin both the state and commercial organizations were used against them in the planning and implementation of the attacks (Bratton, 2009; LaRaia and Walker, 2009; Oh *et al.*, 2011). A considerable amount of the hostile surveillance that is necessary to mount an attack against an urban target can now be carried out using online imaging tools, albeit at a rudimentary level. Information technologies have also provided terrorists with increased communication, as well as surveillance capabilities. Terrorists are able to conceal their planning footprints and train and empower new recruits at a considerable distance. Ultimately, this means that the opportunities for early warnings of impending attacks are partially constrained at the local level, with the security services relying heavily on signals intelligence as a means of identifying potential threats.

The urban context in which these activities occur is itself characterized by points of vulnerability that can be attacked by terrorists. The open and transient nature of cities, the presence of key critical infrastructures and the proximity of large numbers of people in crowded spaces, all combine to present a set of attractive targets for terrorists (Bishop and Clancey, 2008; Boin and Smith, 2006; Fischbacher-Smith *et al.*, 2010; Gilbert *et al.*, 2003; Graham, 2008).

Our aim in this article is to consider the vulnerabilities that exist within hospitals in the United Kingdom. The article frames acute health care within a wider urban context and, in particular, considers its importance as part of the wider contingency response within urban areas, whereby hospitals can be seen as part of the infrastructure that underpins the successful functioning of city life. We also discuss how and why the hospital itself might be vulnerable. A conceptual framework is developed that considers how public organizations, and hospitals in particular, can be vulnerable to attack at multiple levels. These vulnerabilities become represented through gaps in the system that create the potential for failure across layers of the organization. It is in these spaces that hostile actors may seek to expose vulnerabilities in order to cause harm. The article is based on a series of observations made by the authors at several hospitals in the United Kingdom as well as through time spent working within the National Health Service (in one case, as a non-executive director of two NHS Trusts).

IT WOULD NOT HAPPEN HERE, WOULD IT? DETERMINING THE POTENTIAL FOR EXTREME EVENTS

Within many Western societies, there is an assumed level of trust in the generally safe environment that prevails, for the most part, within our communities and cities. So much so that some readers may be confident that the regulatory and policy requirements in place will ensure regular testing of security procedures and that violations of, or gaps within the system, will be addressed by staff at the operating core of the security function. Others will have a belief that no one would ever consider attacking their hospital.

History tells us that our assumptions about likely events are often flawed. For example, the military wing of the Musgrave Park hospital in Northern Ireland was attacked during the 'Troubles' (Hodgetts, 1993); schools have been attacked and children killed by terrorists, fellow pupils and deranged individuals from within the community (Coupland and Meddings, 1999; Cullen, 1996; DeFoster, 2010; Moscardino *et al.*, 2007; Muschert, 2007; Neuner *et al.*, 2009) and the recent attacks in Oslo were initially targeted against government buildings before attention was directed at young people.

The relative ease by which the attackers could access buildings and public areas was a key factor in shaping the fatalities associated with these events. The essentially open nature of public buildings renders them particularly vulnerable to such attacks. Despite a range of mitigation measures (especially relating to vehicles) that have been put in place during the last 20 years, such vulnerabilities remain. To illustrate the ongoing presence of such vulnerabilities, we offer two short vignettes based on our own observations in city-centre hospitals:

1. Several patients with small, wheeled bags were observed walking through the foyer of the hospital. At no point were these patients challenged by security staff regarding the content of their luggage.
2. In a children's hospital, one of the authors was admitted into several locked and restricted areas, having being swiped in by hospital staff past locked security doors and allowed through restricted areas. The basis of this violation of protocol was that the author was en route to a meeting with a senior administrator. The meeting was genuine, but no one asked for identification from the author or sought corroboration from the manager hosting the meeting.

These vignettes illustrate how day-to-day vulnerabilities may give rise to the potential for harm. Essentially, it is often the normality of the process that creates problems for management: such events can pass unnoticed, allowing organizational defences to be bypassed, ultimately resulting in failures that escalate to a point at which managers can no longer control the system (Perrow, 1984; Reason, 1990a, 2008; Turner, 1978).

The focus within the terrorist-related literature is on how health care responds in the aftermath of an attack (Matusitz, 2007; May and Aulisio, 2006). Health care itself tends not to be seen as the target. Hospitals can be seen as potential targets for two main reasons. Firstly, they form part of our critical infrastructure and are invariably a core element in any civil contingency planning process for mitigating the effects of any mass-casualty crisis. Any disruption of the service that they generate will act as a force multiplier for the damage caused elsewhere, i.e. the impact of the attack will be greater than the energy used in that attack.

The role of the doctor in carrying out the attacks on Glasgow airport highlights the role that medical staff can play in such crises (Wessely, 2007). Local hospitals simultaneously became the focus of an active investigation (given that a terrorist had

been a member of NHS staff) as well as a treatment centre for one of those attackers who was injured. This necessitated a heightened level of security within the hospital as a member of staff was placed under armed guard. The potential for confusion within this situation was high as staff sought to comprehend the nature of the event, whilst caring for the attackers and simultaneously recognizing that these perpetrators/patients might leave the hospital open to attack by way of attempted rescue or even retribution. Given the fact that one of the attackers had been a medic, it left open the question of whether they had any collaborators who were also in the health care sector. One immediate result was that health professionals dealing with the injured terrorist were required to work with armed guards present close by. Parts of the hospital were then closed, generating further problems for staff security and safety.

Hospitals are soft targets that are often not adequately target hardened, but are essentially open and porous. Any attacks on their urban catchment areas will see the hospital utilized as a casualty centre and, depending on the nature of that attack, may see people self-presenting, thereby causing congestion and an erosion of the service. A Mumbai-style attack on hospitals could generate mass casualties within a confined space. Hospitals also have within them the means for causing further damage through the presence of low-level nuclear materials. By attacking a hospital directly, it would be possible to have long-term impacts that could make considerable portions of the site unusable for many years and cost large sums to decontaminate.

Our aim in the remainder of this article is to provide a broad framework within which vulnerabilities can be contextualized. In order to explore the implications of such attack strategies for a city – and for hospitals in particular – we will now develop the discussion in the context of an urban environment. Given the obvious sensitivities around the use of a particular town or city as a focus for such discussion, we have a hypothetical but nonetheless realistic urban setting in mind. We frame the specific challenges that may confront a hospital if it were to be directly attacked as part of a wider, and expanding, attack scenario.

CONCENTRATED SPACES: CITIES AS TARGETS

Cities provide a range of targeting choices for terrorists given the concentration of people and buildings, permeable boundaries and transient populations (Amin and Thrift, 2002; Fischbacher-Smith *et al.*, 2010; Libicki *et al.*, 2007). The underpinning transport infrastructures allow large numbers of people to be herded together in ways that not only maximize mobility but also maximize vulnerabilities (Boin and Smith, 2006; Fischbacher-Smith *et al.*, 2010; La Porte, 2007).

We can, therefore, conceive of a city as a set of interconnected nodes and pathways in which people are concentrated, with channels through which they pass, and underlying fabrics that allow a range of transformations to take place (communications, transport systems, infrastructures, etc). The interconnections between these various

elements and layers of a city generate a myriad of opportunities for harm to be created by using the very fabric of the city to cause that harm. Spaces that connect elements of urban life generate 'spaces of destruction' (Fischbacher-Smith, 2011) in which mass-casualty attacks are mounted. These spaces are permeable and vulnerable as they are, by definition, open to public involvement and it is therefore difficult to put robust defence mechanisms in place without changing the nature of the service.

Invariably, military theorists have spent considerable time and effort exploring this vulnerability. We conceptualize the city as a potential series of interconnected zones in which smart target selection can cause a breakdown of the city as a system with a minimum of force (Warden, 2011). Hospitals are part of the very fabric of the supporting infrastructure that exists within cities and provide a range of core underpinning processes by which cities function. A range of public health, primary care, acute and emergency services also keep urban areas (relatively) healthy and disease free. Any erosion of the capabilities to provide health care, would therefore impact on the performance of a range of other services and activities. A city that loses its abilities to contain disease will very quickly start to see a denudation of its core functions as those who provide such service become too ill to work.

Many of the debates around urban terrorism have seen health care's role as dealing with major catastrophic events along with the public health implications of damage to the city's underpinning infrastructure (water, sewage, food provision and power). This traditional emergency-response perspective of health care is one of a contingency bureaucracy (Smith, 1992). Whilst acute care and paramedic services are obvious elements of this process, it is also likely that primary care, the blood transfusion service, coroners departments and mortuary provision, as well as public health, would also play a major role in dealing with the demands of any attack. Hospitals are also functionally dependent on other elements of infrastructure for its routine activities, including power, water, sanitation, IT infrastructure/communications and transport, and any attacks on this supporting infrastructure could severely inhibit hospitals' abilities to function effectively.

Whilst the conventional view sees elements of health care acting as rescuers within an extreme event, they may become victims as the nature of the crisis event escalates. When the World Trade Centre towers collapsed, they claimed the lives of many of those trying to rescue civilians trapped in the burning buildings. The capabilities of New York City to deal with further attacks were, at that point in time, severely degraded through the loss of so many key personnel and the additional task demands generated by the collapse. It raises questions about how a city would cope if those personnel were directly targeted as part of the terrorists' attack strategy.

The fear generated by direct attacks on vulnerable populations would be an important consideration in raising the impact of the event. If hospital sites were attacked as casualties from prior attacks were attending for treatment, then the potential for mass panic would be clearly heightened. Hospitals would, at this point, provide terrorists with a vulnerable and highly concentrated population to attack. In

order to explore these issues in more detail, we need to consider hospitals as potential 'nodes of destruction' (Fischbacher-Smith, 2012) and to frame these nodes as systems in their own right so as to identify failure modes and vulnerable pathways.

HOSPITALS AS NODES OF DESTRUCTION

Health care can be broken down into a set of interactive components. Each component (and their interactions) can generate vulnerabilities, which, if exposed, may cause an organization to fail catastrophically. In keeping with the broad contextual framework of urban areas outlined earlier, we need to consider the interactions between elements of the organization and their associated networks. Our framework draws on five propositions, which are based upon established research in crisis management.

The first proposition is that *organizations incubate the potential for failure based on their routine decision-making processes*. This proposition is based on the work of Turner who argued that the assumptions and core beliefs of managers would shape their perceptions of risk and help to formulate the associated limits of control (Turner, 1976, 1978, 1994). These perceptions then serve to shape the precautionary approaches taken to risk by the organization (Calman and Smith, 2001; Fischbacher-Smith and Calman, 2010; Mitroff *et al.*, 1989; Pauchant and Mitroff, 1992). Any gap between the potential hazards facing the organization and its associated precautionary norms (Turner, 1976) would allow for a crisis to be incubated – that is, the potential hazards will exceed the controls that are in place.

This incubation potential provides the basis for the second proposition that *the potential for failure can be exposed by the actions of individuals at both an operational and a strategic levels*. This proposition is based on the work of Reason (Reason, 1987, 1990b) and others (Collingridge, 1984, 1992; Perrow, 1984; Sagan, 1993; Shrivastava, 1987; Tenner, 1996) concerning the process of human error within systems failure. Errors can be both latent (i.e. they embed failure potential within the system over a long timeframe) and active (where the errors can have a more immediate effect upon performance). The interplay between latent and active errors generates a complex lattice within organizations in which the interactions between different types of errors, operating in different temporal and spatial settings and at different levels of the organization, will generate vulnerable pathways within the system (Smith, 2000).

The third proposition concerns the difficulties involved in managing information flows and making sense of the codified information and early warnings generated around failure (Boisot, 1995; Brookfield and Smith, 2007; Fortune and Peters, 1995). We can frame this proposition in a way that suggests that *organizations experience difficulties in decoding information that is highly codified and which provides early warnings of potential failures*. As a consequence, organizations will often miss the cues that warn them of the potential for failure. Under the conditions of crisis, these issues around information processing become even more acute.

Our fourth proposition is that *the design of organizations and their associated networks ensures that failures will be exposed quickly and possibly over considerable distances from the initiating trigger*. Due to the interconnected nature of modern organizations, a failure in one part of the organization may cascade through the organization bypassing and eroding organizational defences (Van Eeten *et al.*, 2011). The recent financial crisis illustrated the interconnected nature of the system (what Perrow (1984) terms its 'interactive complexity') and how the consequences of the initial erroneous decisions can have consequences for the precautionary norms that are in use within the organization. The speed of that failure cascade can create problems for managers in terms of sensemaking (Weick, 1995, 2001). The closer to the core of an organization where such vulnerabilities are exposed, the greater the potential will be for causing damage across the various interlinked elements.

The final proposition concerns the role of insider threats to service organizations. Having an insider within the organization allows attackers to map the security measures in place, test their robustness and assess how to bypass defences. As a consequence, by being able to deal with the central management or operator elements of the hospital, attackers can create the opportunity to map and expose vulnerabilities. The threat from insiders can be expressed as follows: *service organizations are more vulnerable to the threats from insiders due to their greater reliance on human capital and the need to source the workforce from across society and internationally*. It is this proposition that informs the remainder of this article as a means of highlighting the core vulnerability that exists across health care, namely those who work within it and their potential to cause harm.

THE ENEMY WITHIN: INSIDER THREATS IN A SERVICE ENVIRONMENT

Insider threats are a significant issue for hospitals. The role of doctors in the attacks on the Tiger Tiger nightclub in London and Glasgow Airport leaves little room for doubt that staff working within hospitals have the *potential* to be involved in terrorism (Al-Alawi and Schwartz, 2008; Day, 2007; Wessely, 2007) or other malicious acts (Clarkson, 2001; Donaldson, 1994; Misen, 2000; Rosenthal, 1987, 1995; Smith, 2002). How managers choose to deal with the task demands associated with screening employees has been the subject of considerable attention within government and there have been a range of cases where individuals affiliated with terrorist groups have sought to gain positions within organizations where they could help to plan and carry out terrorist attacks. There are several issues here although perhaps the most obvious relates to the recruitment and selection of staff into the organization.

There have been cases in health care where individuals have claimed bogus qualifications and experience in order to gain employment. This raises the importance of robust screening and background checking processes at the point of recruitment. A second issue concerns those staff who become malicious in their intent after they have satisfied pre-employment checks around qualifications and expertise. The issue of radicalized[1] or

otherwise malevolent staff is a problem that faces many organizations and has recently been the subject of debate, for example, between the government and university administrators in the United Kingdom. It is our contention here that this human component generates a significant vulnerability for hospitals, due to the central role played by people in a service organization, as it allows potential access to a range of critical sources of information within the organization.

Information technology can be a valuable source of intelligence for any attacking group. The ability to access a hospital system (through hacking or employment) provides those who want to attack a system with information on the levels of security, potential access to security codes and access measures, as well as data on the potential storage of hazardous materials on site (bio-waste, nuclear medicine, medical gases and pathogens). Information processing elements of the system could give attackers insights into the likely key nodes (points of attack) and pathways (consequence dynamics of any failure) within the system. Similarly, information about core processes and products, supporting infrastructures and supply chains would allow anyone wishing to attack the hospital system to highlight vulnerabilities, especially through the identification of potential interactions between these various, interconnected, elements of the system.

The customers of the system – in this case, patients and hospital visitors – constitute both a potential target group and a means of testing the permeability of the site. Hospitals are designed to allow people to access many of the core functional areas necessary to provide care. This permeability within the system therefore provides both the opportunity for a mass-casualty event and a means of testing many of the underpinning planning assumptions for such an attack without attracting undue levels of attention.

PHYSICIAN, HEAL THYSELF: DEFENDING PERMEABLE ORGANIZATIONAL SPACE

This article has sought to highlight the threats to hospitals from malicious attacks and the issues that arise from the specific threats associated with mass-casualty terrorism. Whilst it may seem obvious to some readers that hospitals are potential targets, our work with UK hospitals suggests that the threat potential is not something that is high on the managerial agenda. In many cases, the potential for such attacks is often passed on to the contingency planning managers for hospitals rather than featuring as an issue for the senior management board and policy-makers.

There are a number of challenges for policy-makers and for hospital managers that arise from our discussion. Hospital managers must raise awareness amongst staff, patients and the local population, of proportionate risks and of risks that exist but that cannot be accurately predicted. They must nurture the vigilance that provides necessary intelligence to pursue potential terrorists (in advance of an attack) and

simultaneously ensure that patients and staff feel safe. This is especially difficult in the UK setting where medical staff in particular are frequently rotated from one hospital to another, and where the sheer size of a hospital complex means that it is difficult to know who should – and should not – be in the building at any point in time. Moreover, hospitals are caring environments for vulnerable individuals and families and that ethos must be balanced with the need to reduce the vulnerabilities arising from the openness of the hospital system.

Also difficult is the planning of evacuations that would be required following an attack. They are difficult to model given the transient nature of cities and, in holiday periods, the increased tourist population (Fischbacher-Smith *et al.*, 2010). They are equally difficult to rehearse. Communicating risk and communicating emergency plans is exceptionally challenging and yet, the responsibility of hospital managers, and Government is to do just that.

A major challenge at the national and regional levels relates to how government can capitalize appropriately on the lessons to be learned from an event anywhere in the world, and particularly within the United Kingdom. It is often only in the aftermath of events that core assumptions, beliefs and values become challenged such that we begin to see the potential for other extreme events (Fischbacher-Smith, 2010, 2011). Yet, after this initial period of reflection, we often revert to our early position, rendering the event a one-off that will (hopefully) not happen again; a behavioural process that results in a crisis prone culture in many organizations (Mitroff *et al.,* 1989; Pauchant and Mitroff, 1992). As a consequence, organizations often fail to learn from the early warnings or take precautionary action (Turner, 1976, 1978, 1994). Inevitably, managers choose to believe that the controls already in place will do the job that they are designed for and that those responsible for testing those controls do so adequately. The notion of 'it can't happen here' becomes a powerful defence mechanism in shaping the cognitive frames that we use to delimit the boundaries of the risks that we face (Pauchant and Mitroff, 1992).

Hospital management may start with an audit to uncover potential for failure at multiple points in their hospital system and consider the associated implications that exist for their organizations as a consequence. Such an audit represents the first stage in generating the *potential* crisis portfolio, by considering the nature of the vulnerability that exists within the various layers of the organization. The second stage involves an assessment of the networks that the hospital depends upon in order to function – including both human and technical elements – as a means of considering the modes by which those networks can shape failure or serve to help build resilience. Both of these processes will require management to challenge their main assumptions around the nature of vulnerability and the processes by which it can be generated.

The next stage in the process should consider how the hospital's existing defences might cope with the potential threats that have been highlighted in this initial assessment. This needs to be seen as a continuous and iterative process in order to ensure that the organization learns and adapts to the dynamic nature of the threats.

Hospitals specifically need to address several elements of their normal activities if they are to be more robust in the face of potential threats. Hospital boards need to refocus their attention from primarily considering the core business of providing hospital services, to examining potential vulnerabilities, identifying gaps in their systems (strategic and operational) and *testing organizational defences* to ensure that any gaps or weaknesses within the system are addressed. Managers also need to *communicate* the importance of conforming to security protocols in order to raise *awareness* of the potential problems around rogue colleagues or the threats from outsiders. Greater rigour is also needed in relation to *recruitment and selection* of all categories of staff in terms of background checks. Ultimately, the open and permeable nature of health care will remain its main vulnerability. Unless we change the very nature of how we provide care, then such vulnerabilities will be inevitable.

Perhaps one of the greatest challenges to health care managers and to governments, particularly in an evidence-based world, is how to plan for events that have no *a priori* evidence – especially when resource allocation is often contingent on a rational business case. Where there is no evidence for the likelihood of a particular kind of attack, it can be hard for policy-makers or senior managers to engender the kind of serious attention that is required to reshape the thinking within an organization to think of the unthinkable, and to create the capacity to deal with it, and yet to maintain normality in some form of hope for the best but prepare for the worst (Moynihan, 2012). Few organizations have the resource slack for such flexibility.

Finally, a major challenge is for hospital managers and policy-makers to think from the perspective of the attackers when considering emergency planning and organizational security. Attacking a school or hospital seems intuitively objectionable, but such limits may not exist in the mind of the terrorists. Hospital planners need to challenge their own and others' assumptions about where vulnerabilities exist, how (and by whom) they may be exploited and where the vulnerabilities exist within the city system on which the hospital is dependent. In the light of these, and hugely challenging, is their reconsideration of how to ensure security within a health care setting, without compromising freedom, ease of access and the environment and culture of care that such organizations espouse.

A key challenge relates to the timeframe for addressing such concerns in relation to infrastructure investment given that policy-makers must ensure a proportionate response to the risks faced, and yet the timescale for major capital projects is often 10–20 years in a planning cycle. Such a strategic approach to developing resilience will be necessary if government policies in terms of urban protection and health care performance are to have any hope of success. As we noted above, many hospital providers are yet to fully engage in these debates and considerations, both in terms of existing hospital systems and in terms of future hospital service provision, and so further research is also needed to explore managers' and policy-makers' approaches to understand hospital vulnerability to various forms of physical and systems attacks and to the nature of the insider threat.

ACKNOWLEDGEMENTS

The authors thank the editors of this special issue along with the referees for their helpful comments on earlier drafts of this article. The authors acknowledge the funding provided by the EPSRC under grant EPRSC EP/G004889/1 that made this research possible. All errors of omission and commission remain those of the authors.

NOTE

1 In recent years, the focus on radicalized individuals has tended to be associated with Islamic terrorists. However, the term is used here to describe any individual who is inducted into any form of political violence including anti-abortion and animal rights protestors.

REFERENCES

Al-Alawi, I. and Schwartz, S. (2008) Radical Muslim Doctors and What They Mean for the NHS. *British Medical Journal*, 336 pp834.

Amin, A. and Thrift, N. (2002) *Cities. Reimagining the Urban*, Cambridge: Polity Press.

Bishop, R. and Clancey, G. (2008) 'The City-as-Target, or Perpetuation and Death' in S. Graham (ed.) *Cities, War, and Terrorism*. London: Blackwell Publishing.

Bishop, R. and Roy, T. (2009) Mumbai: City-as-Target. *Theory, Culture & Society*, 26 pp263–77.

Boin, A. and Smith, D. (2006) Terrorism and Critical Infrastructures: Implications for Public-Private Crisis Management. *Public Money and Management*, 26 pp295–304.

Boisot, M. (1995) *Information Space: A Framework for Learning in Organizations, Institutions and Culture*, London: Routledge.

Bratton, B. H. (2009) On Geoscapes and the Google Caliphate. *Theory, Culture & Society*, 26 pp329–42.

Brookfield, D. and Smith, D. (2007) Managerial Intervention and Instability in Healthcare Organisations: The Role of Complexity in Explaining the Scope of Effective Management. *Risk Management: An International Journal*, 8 pp268–93.

Calman, K. and Smith, D. (2001) Works in Theory but Not in Practice? Some Notes on the Precautionary Principle. *Public Administration*, 79 pp185–204.

Clarkson, W. (2001) *The Good Doctor – Portrait of a Serial Killer*, London: John Blake Publishing.

Collingridge, D. (1984) *Technology in the Policy Process – The Control of Nuclear Power*, London: Francis Pinter.

—— (1992) *The Management of Scale: Big Organizations, Big Decisions, Big Mistakes*, London: Routledge.

Coupland, R. M. and Meddings, D. R. (1999) Mortality Associated with Use of Weapons in Armed Conflicts, Wartime Atrocities, and Civilian Mass Shootings: Literature Review. *British Medical Journal*, 319 pp407–10.

Cullen, L. (1996) *The Public Inquiry Into the Shootings at Dunblane Primary School on 13th March 1996*, London: HMSO.

Day, M. (2007) Doctors Held for Bombing Attempts, But NHS Defends Vetting Procedures. *British Medical Journal*, 335 p9.

Defoster, R. (2010) American Gun Culture, School Shootings, and a 'Frontier Mentality': An Ideological Analysis of British Editorial Pages in the Decade after Columbine. *Communication, Culture & Critique*, 3 pp466–84.

Donaldson, L. (1994) Doctors with Problems in an NHS Workforce. *British Medical Journal*, 308 pp1277–82.

Durham, M. (1996) Preparing for Armageddon: Citizen Militias, the Patriot Movement and the Oklahoma City Bombing. *Terrorism and Political Violence*, 8 pp65–79.

Field, A. (2009) The 'New Terrorism': Revolution or Evolution? *Political Studies Review*, 7 pp195–207.

Fischbacher-Smith, D. (2010) Beyond the Worse Case Scenario. 'Managing' the Risks of Extreme Events. *Risk Management: An International Journal*, 12 pp1–8.

—— (2011) Destructive Landscapes – (Re)Framing Elements of Risk? *Risk Management: An International Journal*, 13 pp1–15.

—— (2012) 'Spaces of Destruction – Examining the Vulnerabilitiy of Socio-Technical Systems'. Royal Geographical Society-Institute of British Geographers Annual International Conference, 3–5 July, Edinburgh.

Fischbacher-Smith, D. and Calman, K. (2010) 'A Precautionary Tale – The Role of the Precautionary Principle in Policy Making for Public Health' in P. Bennett, K. Calman, S. Curtis and D. Fischbacher-Smith (eds) *Risk Communication and Public Health*. Oxford: Oxford University Press.

Fischbacher-Smith, D., Fischbacher-Smith, M. and Bamaung, D. (2010) 'Where Do We Go from Here? The Evacuation of City Centres and the Communication of Public Health Risks from Extreme Events' in P. Bennett, K. Calman, S. Curtis and D. Fischbacher-Smith (eds) *Risk Communication and Public Health*. Oxford: Oxford University Press.

Fortune, J. and Peters, G. (1995) *Learning from Failure – The Systems Approach*, Chichester: John Wiley and Sons.

Gilbert, P. H., Isenberg, J., Baecher, G. B., Papay, L. T., Spielvogel, L. G., Woodard, J. B. and Badolato, E. V. (2003) Infrastructure Issues for Cities – Countering Terrorist Threat. *Journal of Infrastructure Systems*, 9 pp44–54.

Graham, S. ed. (2008) 'Cities as Strategic Sites: Place Annihilation and Urban Geopolitics' in *Cities, War, and Terrorism*. London: Blackwell Publishing.

—— (2009) The Urban 'Battlespace'. *Theory, Culture & Society*, 26 pp278–88.

Haggerty, K. D. and Gazso, A. (2005) Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats. *The Canadian Journal of Sociology/Cahiers Canadiens De Sociologie*, 30 pp169–87.

Hodgetts, T. J. (1993) Lessons from the Musgrave Park Hospital Bombing. *Injury*, 24 pp219–21.

La Porte, T. R. (2007) Critical Infrastructure in the Face of a Predatory Future: Preparing for Untoward Surprise. *Journal of Contingencies and Crisis Management*, 15 pp60–4.

Laraia, W. and Walker, M. C. (2009) 'The Siege in Mumbai: A Conventional Terrorist Attack Aided by Modern Technology' in M. R. Haberfeld and A. Hassell (eds) *A New Understanding of Terrorism*. New York: Springer.

Libicki, M. C., Chalk, P. and Sisson, M. (2007) *Exploring Terrorist Targeting Preferences*, Santa Monica, CA: RAND Corporation.

Matusitz, J. (2007) Improving Terrorism Preparedness for Hospitals: Toward Better Interorganizational Communication. *International Journal of Strategic Communication*, 1 pp169–89.

May, T. and Aulisio, M. P. (2006) Access to Hospitals in the Wake of Terrorism: Challenges and Needs for Maintaining Public Confidence. *Disaster Management & Response*, 4 pp67–71.

Misen, C. (2000) 'Preface – Shipman's Predecessors' in M. Sitford (ed.) *Addicted to Murder – The True Story of Dr Harold Shipman*. London: Virgin Publishing.

Mitroff, I. I., Pauchant, T. C., Finney, M. and Pearson, C. (1989) Do (Some) Organizations Cause Their Own Crises? Culture Profiles of Crisis Prone Versus Crisis Prepared Organizations. *Industrial Crisis Quarterly*, 3 pp269–83.

Moscardino, U., Axia, G., Scrimin, S. and Capello, F. (2007) Narratives from Caregivers of Children Surviving the Terrorist Attack in Beslan: Issues of Health, Culture, and Resilience. *Social Science & Medicine*, 64 pp1776–87.

Moynihan, D. P. (2012) A Theory of Culture Switching: Leadership and Red Tape During Hurricane Katrina. *Public Administration*, 90:4 pp851–68.

Mulinari, D. and Neergaard, A. (2012) Violence, Racism, and the Political Arena: A Scandinavian Dilemma. *NORA – Nordic Journal of Feminist and Gender Research*, 20 pp12–18.

Muschert, G. W. (2007) Research in School Shootings. *Sociology Compass*, 1 pp60–80.

Neuner, T., Hübner-Liebermann, B., Hajak, G. and Hausner, H. (2009) Media Running Amok after School Shooting in Winnenden, Germany! *The European Journal of Public Health*, 19 pp578–9.

Oh, O., Agrawal, M. and Rao, H. (2011) Information Control and Terrorism: Tracking the Mumbai Terrorist Attack Through Twitter. *Information Systems Frontiers*, 13 pp33–43.

Olson, K. B. (1999) Aum Shinrikyo: Once and Future Threat? *Emerging Infectious Diseases*, 5 pp513–16.

Pauchant, T. C. and Mitroff, I. I. (1992) *Transforming the Crisis-Prone Organization. Preventing Individual Organizational and Environmental Tragedies*, San Fransisco, CA: Jossey-Bass Publishers.

Perrow, C. (1984) *Normal Accidents*, New York: Basic Books.

Reader, I. (2001) Consensus Shattered: Japanese Paradigm Shift and Moral Panic in the Post-Aum Era. *Nova Religio: The Journal of Alternative and Emergent Religions*, 4 pp225–34.

Reason, J. T. (1987) 'An Interactionist's View of System Pathology' in J. A. Wise and A. Debons (eds) *Information Systems: Failure Analysis*. Berlin: Springer-Verlag.

—— (1990a) The Contribution of Latent Human Failures to the Breakdown of Complex Systems. *Philosophical Transactions of the Royal Society of London, B*, 37 pp475–84.

—— (1990b) *Human Error*, Oxford: Oxford University Press.

—— (2008) *The Human Condition. Unsafe Acts, Accidents and Heroic Recoveries*. Farnham: Ashgate.

Rosenthal, M. M. (1987) *Dealing with Medical Malpractice: The British and Swedish Experience*, London: Tavistock.

—— (1995) *The Incompetent Doctor*, Milton Keynes: Open University Press.

Sagan, S. D. (1993) *The Limits of Safety. Organizations, Accidents, and Nuclear Weapons*, Princeton, NJ: Princeton University Press.

Sassen, S. (2010) When the City Itself Becomes a Technology of War. *Theory, Culture & Society*, 27 pp33–50.

Savitch, H. V. (2003) Does 9-11 Portend a New Paradigm for Cities? *Urban Affairs Review*, 39 pp103–27.

Shrivastava, P. (1987) *Bhopal. Anatomy of a Crisis*, Cambridge, MA: Ballinger Publishing Company.

Smith, D. (1992) The Kegworth Aircrash – A Crisis in Three Phases? *Disaster Management*, 4 pp63–72.

—— (2000) On a Wing and a Prayer? Exploring the Human Components of Technological Failure. *Systems Research and Behavioral Science*, 17 pp543–59.

—— (2002) Not by Error, But by Design – Harold Shipman and the Regulatory Crisis for Health Care. *Public Policy and Administration*, 17 pp55–74.

Sorkin, M. (2008) 'Urban Warfare: A Tour of the Battlefield' in S. Graham (ed.) *Cities, War, and Terrorism*. London: Blackwell Publishing.

Tankel, S. (2011) *Storming the World Stage. The Story of Lashkar-e-Taiba*, London: Hurst & Company.

Tenner, E. (1996) *Why Things Bite Back. Technology and the Revenge Effect*, London: Fourth Estate.

Turner, B. A. (1976) The Organizational and Interorganizational Development of Disasters. *Administrative Science Quarterly*, 21 pp378–97.

—— (1978) *Man-Made Disasters*, London: Wykeham.

—— (1994) The Causes of Disaster: Sloppy Management. *British Journal of Management*, 5 pp215–19.

Van Eeten, M., Nieuwenhuijs, A., Luijf, E., Klaver, M. and Cruz, E. (2011) The State and the Threat of Cascading Failure Across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports. *Public Administration*, 89:2 pp381–400.

Vidino, L. (2007) The Hofstad Group: The New Face of Terrorist Networks in Europe. *Studies in Conflict & Terrorism*, 30 pp579–92.

Warden, J. A. (2011) Strategy and Airpower. *Air and Space Power Journal*, 25 pp64–77.

Weick, K. E. (1995) *Sensemaking in Organizations*, Thousand Oaks, CA: SAGE.

—— (2001) *Making Sense of the Organization*, Oxford: Blackwell.

Wessely, S. (2007) When Doctors Become Terrorists. *New England Journal of Medicine*, 357 pp635–7.