Barnes, Paul H. (2008) Evolving issues in Australian Emergency Management. In *Australian Security Magazine*, Yaffa Publishing.

`

Evolving issues in Australian Emergency Management

2,380 words

Natural hazards have created significant disturbances across wide areas of Australia with seasonal flooding, bush fires and drought as matters of common historical and recent fact. The potential for increased frequencies of natural disasters linked to climate change adds further complexity to this mix. Technical incidents have also caused significant disruptions. Incidents such as the ‘Coode Island Fire’ and the ‘Longford Gas explosion’ in Victoria, with its long and difficult social consequences, come to mind. In addition to these more ‘familiar’ threats (natural and technical) concern about emergent and re-emergent disease, animal and plant biosecurity issues and the uncertainty of bio-terrorism have been to the fore. All of these concerns have made ensuring effective emergency response capabilities both regionally and nationally, critically important.

But how effective is the Australian emergency management system? Is it equipped to deal with a Hurricane Katrina-style disaster? Much has been made of the failure of the U.S. administration(s) following Hurricane Katrina. Congressional testimonies and other post-incident assessments have identified issues such as insufficient and untimely communications to the President (thus not allowing a timely activation of appropriate federal responses) and for slow and initially unfocussed regional and local responses to the event. Other sources have identified a strong contributing factor to the severity of the impact and consequences from cumulative environmental degradation of the Florida wetlands (thus decreasing the capacity to slow down and absorb the flood surge) in addition to design faults and lacklustre upkeep of levies (originally designed and maintained by the Army Corp of Engineers). It is interesting to note that the Commander of the U.S. Army Corp of Engineers resigned post-Katrina but much later in the recovery phase with much less fanfare than the Director of the U.S. Federal Emergency Management Authority.

Differences exist between Australia and the United States in relation to the operational and organisational structure of emergency management and the level of control for emergency response: municipal in the U.S. and state-based in Australia. Both countries, however, have a federal level institution that coordinates emergency response resources and support when an emergency event outstrips state-based capacities. While Australia does contend with cyclones (of a similar size to Katrina) I don’t believe that we would face the same scale of aftermath seen in New Orleans for a number of reasons: one being the different demographics, urban density and land use of northern Australia. While considerable damage was inflicted on infrastructure and housing and building stock in 2006 by Cyclone Larry, population factors and much lower urban densities resulted in comparatively less damage and social disruption than in New Orleans. A further factor with Cyclone Larry was that the initiation of a multi-agency response (albeit a standard practice) was rapid with significant coordination protocols enacted within hours of the storms transition inland.

There is of course a deep experience of preparation, response, and recovery from conventional disaster events in Australia embodied in the well-established protocols of the emergency service agencies and state-based disaster coordination groups that include representatives from the police, Australian Defence Force, government agencies and of course the insurance industry. Australia also has uniform standards and capabilities across our states and territories. Peak industry institutions such as the Australasian Fire Authorities Council facilitate conformity and capacity building via representation of all state fire authorities as well as government departments working in land management. Other institutions, such as the Australian Building Codes Board, oversee regulation issues of health, safety, amenity and sustainability in buildings via nationally consistent building codes, standards, regulatory requirements and regulatory systems. Similar coordination exists nationally regarding ambulance services, and importantly, diagnostic public health laboratory networks.

Of course any escalating crisis or large disaster will put intense strain on state-level capacities and rapid federal-level intervention would be needed. This is of nothing new to Australian experience and in fact for many likely crisis events guidelines and protocols for rapid and coordinated emergency response have been in place for considerable periods of time. Never-the-less significant crises flowing from bio-security incidents impacting on humans, plants or animals would be draining on resources and test the endurance of response agencies.

Other categories of incident, contextually different to the ‘hot pursuit’ crises mentioned above, exist and require different ways of analysing the potential for loss, extent of disruption and options for initiating response and recovery. A generic instance of this category derives from the increasing hyper-complexity of embedded information-communications-technology (ICT) in essential services and emergent inter-dependencies within and across systems of infrastructure. Uncertainty inherent in such systems can create significant challenges in governance for the private and public sector alike. Unmitigated disturbances are likely to generate cascading impacts propagated along unexpected pathways and fault lines throughout commercial and institutional segments of established and establishing economies. The potential for rapid spread of consequences, geographically and virtually, can render a comprehensive understanding of such an emergency beyond the grasp of competent authority.

Because of these cascading phenomena, institutions would be unlikely to face single incidents but rather series of systemic failures: often appearing concurrently. A further point to note is that both natural and technological hazards can impact directly on socio-technical systems as well as being propagated by them: as *critical network events*. Such events have been described as ‘outside of the box,’ ‘too fast,’ and ‘too strange.’ Emergent complexities in linked systems often make crises difficult to anticipate and consequences difficult to plan for. Further, under emergency conditions, the pressure on senior decision-takers to ‘make-sense’ of multiple lines of information (for both crisis and consequence phases) is significant. Examples of this category include the spread of (bogus?) white powder letters through national and international postal systems and airline travel as a technical vector for the movement of emergent human disease.

Another example of the *network event* category emerges as disruptions in supply chains and supportive logistic systems and the porosity of trade barriers. The global economy relies on the efficiencies of transactions across these borders. Vulnerabilities within supply chains are generally poorly understood and managed, partly because stakeholders function at varying levels within commercial systems: as retailers, wholesalers, suppliers, manufacturing enterprises and governments. Causal factors are obscured in these contexts due to varying scales over which stakeholders operate. The process of how to mount an emergency response to recover a disrupted supply chain is not, therefore, a simple undertaking. This type of problem is being examined by elements of the Asia-Pacific Economic Cooperation (APEC) Counter Terrorism Task force.

Not-with-standing the effectiveness of our emergency management systems there are evolutionary steps that warrant further consideration: particularly in relation to networked crises. These range from variation in conceptual underpinnings to enhanced scope of coverage for emergency management activities.

Initially, it is useful to re-examine the well established and successful operational framework for defining pre and post-incident stages of emergency management. Namely:

- **Prevention** - recognition systems for emerging crises;
- **Preparation** - planning for the unknown;
- **Response** - making effective decisions and having them implemented; and
- **Recovery** - restoring normality and learning.

Both *preventing* and *preparing* for emergency situations presumes a comprehensive knowledge of the factors and conditions that can manifest during an emergency and how they might directly or indirectly exploit organizational and institutional vulnerabilities. *Responding* and *recovering* from emergencies also assumes an effective appreciation of mitigation and consequence factors. This level of understanding presumes planners, advisors and responders can make-sense of confusing and at times conflicting information flows: a presumption that many iconic disasters have shown to be unsupported. Such a situation would also be pertinent in a ‘network event’ as described earlier.

Two key capacities would enhance an organisational repertoire in such situations. These are the application of foresight to crisis incidents and robust analytical and conceptual frameworks of security and emergency risk management.

While notions of foresight are *pre-incident*, as is intelligence-driven risk management, emergency management, per se, may not be so. Even though uncertainty is a significant factor, commentators in the early 1990's suggested that many organisational crises (and by association emergency incidents) may replicate in a number of common ways, yet never manifesting in exactly the same manner. The suggestion that there are repetitive and recognizable stages in major socio-technical failure is compelling and is supported by a substantial literature grounded in the analysis of industrial and organizational settings over a number of years. Key findings from a selection of this literature identify five stages in [organisational] failure that are particular to many complex emergencies. These stages being:

- ***Pre-conditions*** - sets of operational activity where 'signs' were buried or ignored in background noise;
- ***Trigger*** - an escalation factor either internal or external to an organization or setting;
- ***Crisis*** - an emergent process exhibiting uncertainty and potential for loss and/disruption;
- ***Recovery*** - systems recovery and normalization of functions;
- ***Learning*** - identification and changes to functional capacities of organization/systems.

If analytical capacities that addressed these stages were to be embedded in an organisational repertoire, enhanced resilience to disruptive events should follow. Resilience in this sense has been defined as the capacity of a system to maintain functionality and output when exposed to disturbance. While early notions of resilience emerged from ecology in the 1970's it's viability in the analysis of socio-technical systems has become important in recent times. An 'adaptive' capacity is an element of the resilience concept that can focus on the 'learning' and vulnerability-reducing capacities of institutions, regulatory bodies and, of course, emergency response agencies.

Central to the notion of resilience from a national security perspective and for critical infrastructure protection in particular is an appreciation of the vulnerabilities within a system exposed to known or suspected threats and an assessment of the likelihood that such threats might manifest as harm. Vulnerabilities might equally be examined from the perspective of complexity and the inter-connectedness of infrastructure systems - whether concentrated or geographically dispersed. These factors often make effective governance and sustained availability and reliability of essential services problematical.

Supporting resilience is an important business continuity management and emergency management outcome. A greater appreciation of resilience factors across all segments of societal infrastructure would benefit both the public and private sectors and enhance effectiveness of emergency response capability. Specific needs exist including:

- The design of frameworks of asymmetric threat recognition and response capacities;
- Processes for continual and adaptive vulnerability analyses within and between complex and critical infrastructure systems;
- An ability to anticipate counter-intuitive triggers of loss-causing incidents (tipping points);
- Continuity planning methodologies that integrate the functionality of complex infrastructure systems;
- Conceptual understanding and tools to anticipate emergent threats that exploit systemic vulnerabilities

Addressing the needs outlined above would allow decision makers, in both affected institutions and emergency response organisations, to make better 'sense' of complex emergency events and enhance response, recovery and learning outcomes. Such sense making capacities would logically allow:

- Enhanced assessment of the plethora of data and information generated during emergencies *(Without filtering important data);*

- Development of Scenarios (speculation) about cascading impacts through time;
- Identification of critical dependencies in human/built environment & biological systems that might mitigate or exacerbate consequences;
- Examination of *what if*, *how could* and *what when* questions;
- Assessment of asymmetric threats.

Future issues

If Australia is to maintain a capacity for emergency management that can enhance societal resilience, then relevant institutions must be enabled to maximise service delivery even when faced by many types of threat. A comprehensive all-hazards approach that includes coverage of emergent and novel threats would entail institutional and procedural design that makes efficient and effective use of a full range of information sources available: a true data fusion. There is a clear role for private sector providers of hardware and software systems in such decision support roles, particularly in the novel use of Geographic Information System capabilities. Of course such a goal for emergency management decision making support is not viable without support in policy and governance at State, intra-State and Federal level. Such a goal would also include potential collaboration with the private sector – not only because significant amounts of infrastructure is owned or operated by this sector. While actual privatised first responder capacities in wider community settings seem unlikely into the near future, beyond specialist roles in some industrial settings, a foreseeable role does exist in threat and risk-based decision support roles. It is notable that the Director-General of ASIO recently flagged an increased role for the private sector in assisting with the provision of intelligence related advice. This linkage is also likely to be bi-directional in that agile business decisions need good information and under current global conditions this would also mean access to appropriate threat assessments.

There are also strong signs of a more eclectic approach to research and development across the emergency management sector. An example of this is in the form of a Cooperative Research Centre (CRC) funding re-bid by a consortium led by AFAC (following on from the current Bush Fire CRC). This new CRC aims at broadening its focus to include 'public planning policy and critical infrastructure protection' issues: in addition to other areas such mitigating impacts of climate change.

A comment from the '9/11 Report' by the National Commission on the terrorist attacks in the US in 2001 provides an interesting context for considering future needs in the Australian context. It suggested that there were four kinds of failure in terms of governance with respect to the event itself: problems in imagination, policy, capabilities, and management. While all four are important I suspect that the first of these points is the most critical. Beyond mere failure of imagining what could happen and how likely an incident could be, or even 'joining the dots,' failure to anticipate need (derived of course from a comprehensive knowledge base), limits both quality and depth of emergency-related policy development, capability maintenance and management. Attention to all four of these failure points will be needed in Australia if the benefits of a resilient society are to be pursued.

Finally, a current and future challenge faced by emergency managers in both the public and private sectors is the avoidance of investing in capacity and capability based on past success - or failure. In other words effective emergency response must not be predicated on propensities to respond to past emergencies. A capacity to anticipate emerging threats and systemic vulnerabilities is critical.

Bio:

Dr Paul Barnes teaches and carries out applied research on Crisis Management and Business Continuity Planning in Socio-technical systems in the Faculty of Business at the Queensland University of Technology, Brisbane. Before returning to academia he held public sector positions in Emergency Management and Corporate Risk Management at State level and Security Policy Development within the Australian Department of Defence.