ORGANISATIONAL RESILIENCE

Understanding the Concept and its Application

A strawman paper by Alastair McAslan
Director of the Torrens Resilience Institute, Adelaide, Australia
3 May 2010

Abstract: The concept of organisational resilience is new to management thinking. It suggests an ability of organisations to recover and return to normality after facing an alarming and often unexpected threat. The paper considers changes to the form, scale and impact of threats facing organisations in Australia today, as well as longer term challenges such as global warming and the increasing fragility and expectations of today's society. The general principles and requirements of organisational resilience are explained. These include: (1) the need for managers to understand better the organisation, its environment and critical business processes; (2) the suitability and completeness of the organisation's resilience policy and continuity plans; and (3) the organisation's willingness to implement, and if necessary to adapt, its policy and plans for prevention, mitigation, response, continuity and recovery. The paper suggests that organisational resilience does not replace risk management or continuity planning; rather, resilience should be seen as an organisational goal, whereas risk management and continuity planning are management tools. The challenge facing us now is how best to develop and promote organisational resilience in a way that assists government to develop policy and enables managers to build organisations which are able to operate more effectively and confidently in our increasingly volatile, uncertain, complex and ambiguous world.

Key words: Resilience, risk, vulnerability, adaptability, business continuity

INTRODUCTION

Managers are constantly striving to improve the performance of their organisations. Regardless of the type and purpose of an enterprise, its leaders seek to enhance the way an organisation conducts its business by adopting management practices which aim to increase effectiveness, efficiency and safety.

In the 1970s and 80s, many organisations embraced the concept of quality. New terms, procedures and tools such as Total Quality Management and Six Sigma were developed, and international quality standards were introduced. The purpose of these tools and standards was to improve the ability of organisations to produce goods and deliver services which satisfied the customers' needs and expectations. In the 1980s and 90s, risk management was promoted from the disciplines of engineering and insurance to centre stage of management practice. The move to systematically assess and mitigate risk was a response to new health and safety legislation, tighter regulation and the growing cost of insurance. But it also reflected a change in business attitude where managers recognised they could obtain competitive advantage by better understanding and treating risk.

Events such as the catastrophic failure of the Challenger space shuttle in front of a global television audience, extreme weather events such as the 2004/05 South Asia tsunami, the threat of BSE (mad cow disease) and flu pandemics, the institutionalisation of terrorism and the rapid onset of the 2008/09 global financial crisis have all contributed to a heightened awareness of personal risk and organisational vulnerability. Paradoxically, this increased awareness of risk and vulnerability has been accompanied by a trend to achieve greater organisational leanness and efficiency, which in turn has led to more brittle and vulnerable enterprises. Companies have stripped away layers of management in an attempt to streamline their organisations and reduce costs, and they have outsourced non-core business processes to external providers. Supply chains have been stretched to the limit, goods are sourced from ever more distant locations and levels of inventory have dropped to a matter of days, or in some cases to a few hours.

The powerful combination of highly visible threats, reduced redundancy and reserves, and a growing reliance on extended supply chains and sub-contractors has encouraged managers to embrace concepts such as enterprise risk management and business continuity. More recently, the term *organisational resilience* has been introduced as a management concept to describe the ability of organisations to cope in the face of adversity – to recover and return to normality after confronting abnormal, alarming and often unexpected threats.

This paper considers the form and impact of current risks facing organisations and longer term challenges such as global warming, an aging population and changes to society's needs and expectations. The paper defines *organisational resilience* and assesses its utility as a management concept to be used by policy makers and practitioners.

THE STRATEGIC AND OPERATIONAL ENVIRONMENT

The threat from natural disasters, health pandemics, IT fraud, terrorism and other disruptive challenges including the recall of faulty and potentially dangerous products has increased significantly in recent years. Indeed, 24 hour television news, mobile phones and social networking have made us more aware of potential threats, and changes to society have made us feel more isolated and vulnerable.

While managers must be ready to address such high-impact events, there are many less newsworthy risks that can be equally damaging to the wellbeing of an organisation. According to the US National Archives and Records Administration, 25% of the companies that experienced an IT outage of two to six days in 2007 went bankrupt immediately. The same study shows that 93% of companies which lost their data centre for 10 days or more filed for bankruptcy within a year. (IBM, 2009, p.2)

In a survey by the Economist Intelligence Unit, organisations reported a wide range of concerns ranging from the spectacular to the mundane. (EIU, 2007) Loss of data and human error are seen as the most likely threats, whereas more catastrophic events, such as natural disasters, terrorism and pandemics, come further down the priority list; see Figure 1.

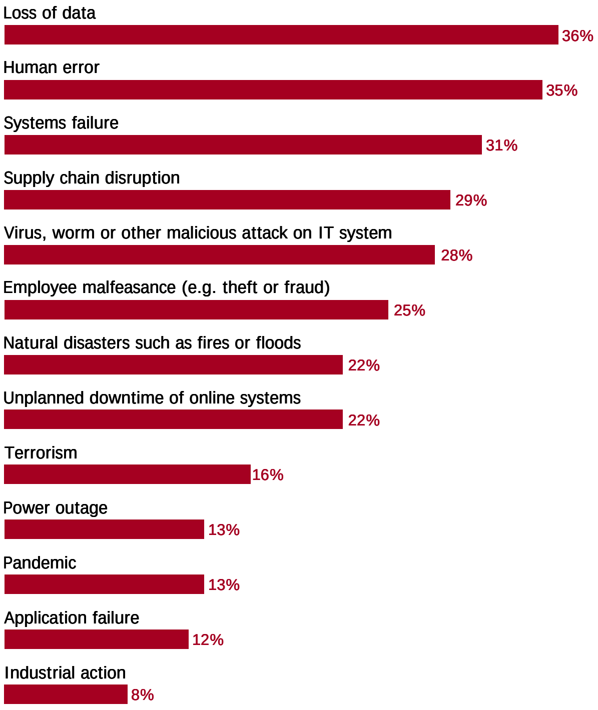

Figure 1: Perception of threats facing organisations (Economist Intelligence Unit survey, 2007)

There is a growing demand for authoritative assessments and studies on risk and future threats. Organisations such as Reuters, the Rand Corporation, Deloitte, EIU, KPMG, Swiss Re, Morgan Stanley, McKinsey and international bodies such as NATO and the World Bank assess trends and identify potential tipping points which may lead to disruptive challenges. They analyse risks and develop scenarios ranging from increased regulation to currency collapse and assess their likely probability, impact and intensity. New risks are added as they emerge, replacing threats that have diminished.

Each year a report is prepared for the World Economic Forum (WEF) on global risks. The report outlines the issues most likely to impact on governments and organisations, and makes recommendations on actions required. A theme which has been repeated in recent reports is the recognition that global risks are complex and interconnected.

Shocks and vulnerabilities are truly international, even if the impact and response may differ at the local level. This recognition is illustrated by the number of linkages in the WEF 2010 Risks Interconnection Map (RIM). Figure 2 shows the top-level perspective of the RIM; each risk (node) has its own map which goes into much greater detail.

The 2010 report highlights the threat from slow onset risks such as global warming, population growth and ageing. While sudden shocks can have a huge impact, be they serious geopolitical incidents, terrorist attacks or natural disasters, the report suggests that "…. the biggest risk facing the world today may be from slow failures or creeping risk." (WEF, 2010, p.5) Because these failures and risks emerge over a long period of time, their full impact and long term implications can be vastly underestimated. Cork et al. (2009) suggest that paying insufficient attention to slow change has resulted in ineffective or delayed policies for dealing with some social, economic and environmental issues in Australia such as water use, salinity and biodiversity.

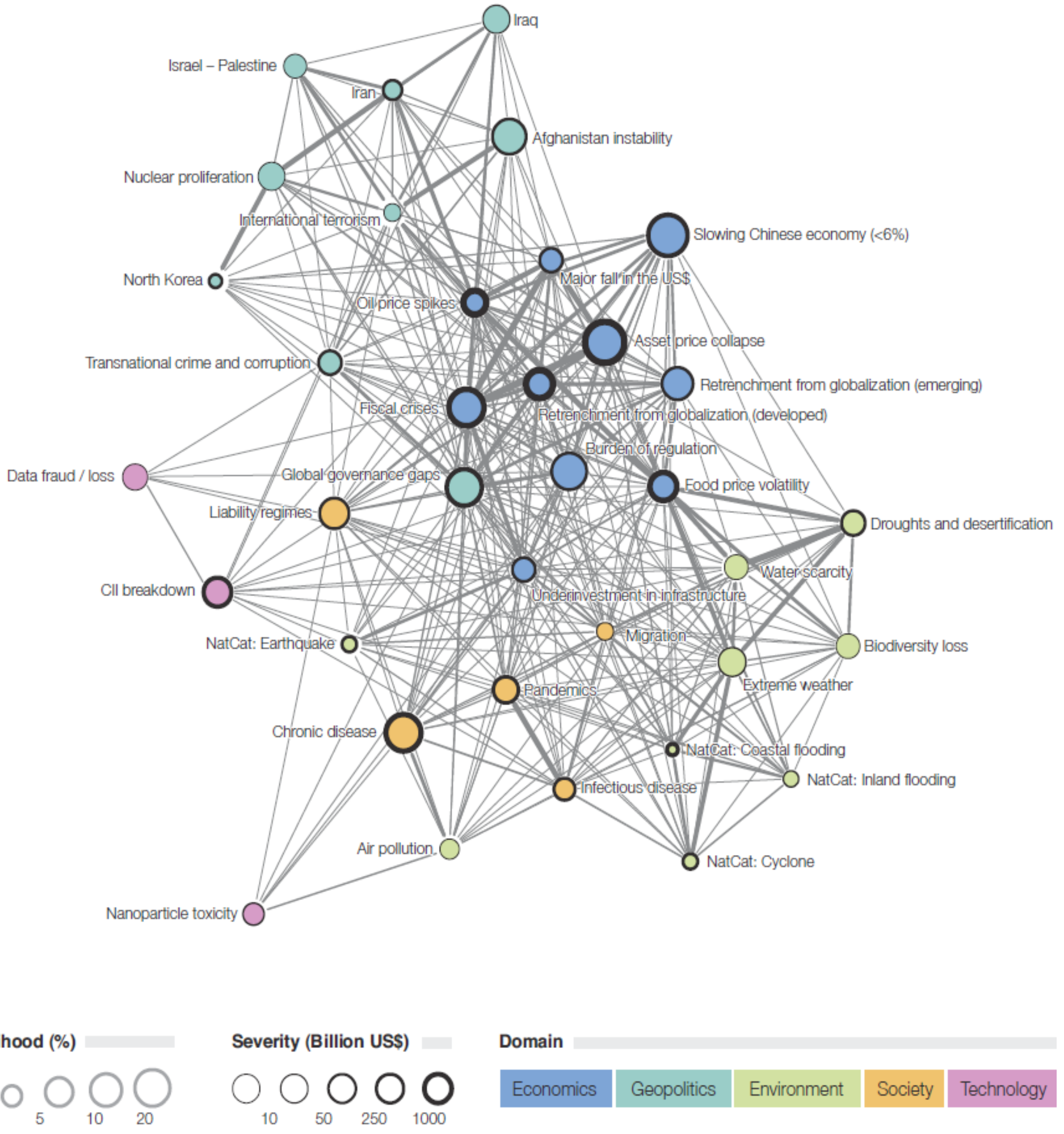

Figure 2: WEF 2010 Risks Interconnection Map

LONG TERM CHALLENGES - EMERGING TRENDS

Although such studies and reports provide governments and organisations with greater understanding of the form and interconnectedness of potential risks, they cannot predict the future with any certainty. There are, however, a number of emerging trends and characteristics of a future world which planners must recognise as potential threats in developing their mid to long-term organisational strategies.

Financial instability

The impact of the 2008/09 financial crisis has been profound. In bailing out major banks and iconic companies, governments have assumed unsustainable levels of sovereign debt, which in turn has impacted on organisations trading within, from, and to such countries. Some governments have resorted to "quantitative easing" to stimulate their economies by purchasing financial assets such as corporate bonds from the banks using money created *ex nihilo* (out of nothing). Such policies aim to keep the economy moving by encouraging financial institutions to lend money to businesses. But the printing of government money could lead, in the worst case, to hyperinflation as well as further increasing the levels of sovereign debt.

A report prepared by a Commission of Experts for the UN General Assembly in September 2009 concludes that the global financial crisis has exposed fundamental problems, not only in national regulatory systems affecting finance, competition and corporate governance, but also in the international institutions and arrangements created to ensure financial and economic stability. The US Institute of Internal Auditors note that ".... too many organisations turned a blind eye to red flags, failed to effectively manage enterprise risks, and demonstrated a greedy mindset that tolerated and exacerbated unprecedented debt. And as a result, market volatility, lack of liquidity, rising unemployment, and record-low consumer and business confidence are the price we are all paying." (IAA, 2009, p.2)

Although Australian banks were not affected by toxic debt to the same degree as the US and many European banks, Australia cannot avoid the economic turbulence being felt in the rest of the world. The current economic volatility and uncertainty represents the greatest immediate risk to most organisations in the developed world.

Climate change

There is overwhelming evidence that our climate has been changing over the past hundred years and will continue to change, although there is debate on the contribution of greenhouse gasses resulting from human activities. Climate change is a pervasive and critical issue for Australia. Statistics provided by the Government's Bureau of Meteorology show the national mean annual temperature has increased since 1950 as have the ocean temperatures around Australia, most notably the Tasman Sea. Although the total annual rainfall shows a moderate rise, there has been a significant increase in year-to-year volatility, with rainfall trends varying between regions and seasons. In the future, Australia can expect more extreme events to occur which will impact on organisations, communities and individuals - unless significant climate change adaptation strategies are adopted.

The Rudd Government's position paper on *Adapting to Climate Change in Australia* published in February 2010 acknowledges that we are already experiencing the early effects of climate change. The paper notes that "…. many scientists now believe the climate system appears to be changing faster than earlier thought likely, and the risks associated with the upper range of the Intergovernmental Panel on Climate Change (IPCC) projections need seriously to be considered." (Australian Department of Climate Change, 2010, p.4) Even if global warming can be contained to around 2ºC, Australia will have to manage serious risks from climate change. The Government recognises that ".... most of the assets and activities at risk are owned or managed by businesses and the community. It is therefore reasonable to expect that much of the national effort (to mitigate the associated risks from climate change) will be taken by businesses and communities. It is not feasible for governments to bear all the costs." (Australian Department of Climate Change, 2010, p.22)

Population growth

After growing very slowly for most of human history, the world's population more than doubled in the last half century to reach 6 billion in late 1999. By 2006 it had reached 6.7 billion. Lower mortality, longer life expectancy and a youthful population in countries where fertility remains high all contributed to the rapid population growth. According to the United Nations, the world population is expected to rise by a further 2.5 billion people, to reach a total of 9.1 billion in 2050. The increase alone is close to the total world population in 1950. Most of the growth will take place in the less developed countries, and will be concentrated among the poorest populations in urban areas. (UNFPA, 2009)

By contrast, the overall population of the more developed countries is likely to show little change over the next 40 years. Fertility is below two children per woman in all 45 developed countries or areas, as well as in 28 developing countries including China. The population of developed regions is aging and would actually decline were it not for migration. The Australian Government's Intergenerational Report (2010, p.vii and p.1) suggests that by 2050 there will be only 2.7 people of working-age for each citizen over 65. Currently there are 5.0 working-age Australians for every one over 65; four decades ago there were 7.5. Over the same period, the Government of Australia envisages the population will grow from 22 to 36 million. Prime Minister Rudd has suggested that "…. unless we make big changes, we will either generate large, unsustainable budget deficits in the second quarter of the century, or else we'll need to reduce government services, including health services, as the needs of an ageing population become greater." (Government of Australia, 2010, p.7)

The implications of an aging population on organisations will be substantial in terms of employee costs, flexibility and availability, and it will make Australian businesses less competitive. An expanding population will also increase pressure on the country's infrastructure, in particular on housing, health and schools, and the supply of water for domestic use and businesses.

Uncertainty

In the eighteenth century, social theorists thought the laws of human behaviour were governed by causal laws, like Newtonian physics and quantum mechanics. It has since become clear that no deterministic laws govern societies' actions, including those of organisations. Yet, as Adam Gordon suggests in his book *Future Savvy*, our lives and decisions are dominated by statistics. "For better or worse, quantitative analysis has become the authoritative form of knowledge …. Economics, once an area of social analysis has become a field of turbo-maths, while management academics produce papers that more closely resemble particle physics than anything real managers actually do." (Gordon, 2009, p.156) Ready access to IT has encouraged such an approach and many organisations look to computer-driven modelling to predict future outcomes.

In practice, we cannot predict the future with any certainty or confidence using data, algorithms or computer programs alone. Chaos theory, which has migrated from the natural sciences to economics and the social sciences, helps explain the difficulties in forecasting the future. Chaos theory also explains how apparently inconsequential events can influence strategic outcomes. The increasingly complex, interconnected and rapidly changing environment is described by US military planners as VUCA (volatile, uncertain, complex and ambiguous) – an acronym which seems equally appropriate to describe the situation facing many organisations today in the private, public, not-for-profit and non-governmental sectors. (US Army War College, 2004)

In an attempt to provide some clarity to the VUCA vision of the world, McKinsey (the international management consultancy company) use an analytical framework involving four levels of uncertainty based on the ideas of Courtney et al (1997). Level 1 refers to slow-moving, well established situations where outcomes are dependable; this is characterised by a "mature industry" with a stable set of competitors, no anticipated regulatory changes, short and reliable supply chains, and satisfied customers. Level 2 refers to situations where there is a limited set of future outcomes depending, for example, on the pending award of a major single contract; such situations are common in the aerospace and defence sectors. Level 3 refers to situations where outcomes are indeterminate but bounded within a plausible rage of conditions, and where implausible or impossible outcomes can be identified and discarded. Level 4 refers to highly complex, ambiguous and volatile situations where outcomes are unknown, and a limitless range of outcomes is possible. The level of uncertainty increases with the degree of complexity and pace of change. It also increases over time. The further into the future we look the higher the uncertainty.

Such analytical frameworks enable managers to understand the degree of uncertainty and to apply appropriate tools. Market research and Porter's Five Forces model, for example, can be used for Level 1 organisations; classic risk management tools, advanced quantitative techniques, decision trees and probability-based calculations can be used for Levels 1 and 2; scenario planning can be used for Level 3; and gaming can be used for Level 4.

Needs and expectations of society

Perhaps the greatest challenge facing governments, organisations and communities today is satisfying society's needs and expectations in the event of a disaster, or indeed the fear of some future disaster. Robert Putman, in his influential paper *Bowling Alone* (1995) identified changes in the way Americans relate to one another in the workplace and through clubs and societies. He observed a lack of civil engagement which undermined community and organisational identity and cohesion, which in turn reduced the nation's ability and willingness to recover after confronting abnormal, alarming and unexpected threats.

Heartfield (2002) suggests that society's ".... more diminished and more isolated, sense of self" has altered our confidence to deal with change and the problems it creates. In our technically networked world we may be more aware, but we are also easier to scare. Being more isolated leaves us more self-centred, as well as risk averse. Durodié (2005, p.17) goes further by suggesting that our politicians have become ".... societal risk managers around issues such as security, health and the environment. They pose as the people who will protect us from our fears and regulate the world accordingly." He argues that the more such concerns are highlighted, the more difficult it becomes for authorities to satisfy the insecurities they drive.

Over the past few decades we have benefited greatly from improvements to our health and safety, and we look to our governments and others in authority to mitigate threats and remove risks. We demand information, guides, standards and regulations to assist us reduce the likelihood and consequences of a disruptive event, and we expect financial support to enable us recover as quickly and completely as possible. There is little evidence to suggest that society, at least in the Developed World, will revert to the norms of earlier times and accept greater personal and collective responsibility. Indeed, Furedi and Roberts (2004, p.8) suggest that self-reliance is old fashioned and self-seeking is now actively promoted, and ".... for whatever self-intentioned reason we are unlikely to see a truly resilient society emerge."

Others are less pessimistic. On 4 December 2008, in his first national security statement to Parliament, Prime Minister Kevin Rudd stated that ".... one of the fundamental assets we have .... is our underlying strength, resilience and cohesion as a nation .... in Australia we have a strong tradition of volunteering support to our communities, especially in times of emergency, demonstrating the innate resilience and collective responsibility we all share as Australians." Others agree. "Ordinary human beings are at their most social and rational in a crisis. It is this that should be supported, rather than subsumed or even subverted." (Durodié, 2005, p.19)

SECURITY, RESILIENCE AND ROBUSTNESS

Redefining security

In 2004, the British Government introduced a revised Civil Contingencies Act. In a consultation document which preceded the Act, Douglas Alexander, then Minister for the Cabinet Office, stated that "…. many of the certainties that determined the way in which the public, private and voluntary sectors prepared for past emergencies cannot now be relied upon. Civil defence no longer exists as a practical stand alone activity. Traditional emergency planning needs to be more flexible, and have greater regard to risk management. A new framework (which encourages the building of resilient communities and organisations) is needed to build a wide range of coordinated responses." (UK Cabinet Office, 2003)

The US Department of Homeland Security has also embraced the term resilience, and sees the concepts of resilience and national security as complementary. A recent report prepared by the National Infrastructure Advisory Council on *Critical Infrastructure Resilience*, stressed the importance of resilience in the protection of the nation's infrastructure "…. because (the concept of resilience) recognises both the need for security and the reliability of business operations in the US." (NIAC, 2009, p.6) The report concluded that "…. the challenge facing Government is to maintain its role in protecting critical infrastructures, while determining how best to encourage market forces to improve the resilience of companies, provide appropriate incentives and tools (including national standards) to help entire sectors become resilient, and step in when market forces alone cannot produce the level of security needed to protect citizens, communities and essential economic systems." (NIAC, 2009, p.10)

In his first national security statement to Parliament in December 2008, Prime Minister Kevin Rudd defined the security of Australia and its people in a broad sense to include threats to human security other than attacks from foreign states and terrorist acts. He stated that such non-traditional threats include attacks on critical infrastructure and information systems, transnational crime and the impact of climate change which may bring unregulated population movements, declining food production, reductions in arable land, violent weather patterns and resulting catastrophic events. More recently, the Council of Australian Government (COAG) agreed a range of measures to strengthen the country's capacity to withstand and recover from emergencies and disasters by adopting "…. a new whole-of-nation resilience-based approach to natural disaster policy and programs." (COAG communiqué, 2009)

What is resilience?

Resilience is the ability of something or someone to cope in the face of adversity – to recover and return to normality after confronting an abnormal, alarming, and often unexpected threat. It embraces the concepts of awareness, detection, communication, reaction (and if possible avoidance) and recovery. These are essential features of the daily struggle for life and are founded in our basic instinct of survival. Resilience also suggests an ability and willingness to adapt over time to a changing and potentially threatening environment.

The concept of organisational resilience was first used to describe the need for companies to respond to a rapidly changing business environment. In their paper *The Quest for Resilience*, Hamel and Välikangas (2003) argued that successful organisations were those who understood the dynamic nature of their business environment (competitors, technology, the availability and cost of finance, government policy, and their customers' needs and expectations) and who were able and willing to adapt to sudden and large changes to the environment.

Over the past five years or so, the concept of organisational resilience has expanded its focus as organisations in the private and public sectors have redefined the extent and scope of the threats facing them. As stated earlier in this paper, as our society becomes more complex and interdependent we are becoming more vulnerable to disruptive events from a broad range of threats and hazards. If not properly managed, a disruptive event can escalate into an emergency, crisis, or even a disaster. It can taint an organisation's image, reputation or brand in addition to resulting in significant physical damage, injury or loss of life.

The aim of building resilience is to remove or reduce the exposure of organisations to threats and hazards by developing protective measures which aim to reduce the likelihood and consequences of a disruptive event, by prevention when possible, responding effectively and efficiently when an event occurs, and by recovering as quickly and completely as possible. For commercial enterprises, the need to be resilient is driven by competitive market forces "…. because customers and shareholders expect products and services to be delivered despite disruptive events." (NIAC, 2009, p.9)

Robustness: an achievable goal?

It is important to note the difference between *resilience* and the concept of robustness. Robustness is the ability of a system to maintain its functions and characteristics in the face of disruptive events. A robust organisation should be able to withstand all external shocks with little or no impact on its organisational structure, people, physical assets and IT systems, and be able to meet its operational targets as well as achieve its strategic objectives. (Cork et al, 2008, p.5)

In contrast, a resilient organisation recognises that some of its functions and characteristics may be affected by some disruptive events. It will retain an ability to achieve its long term strategic objectives although it may fail to meet some short term operational targets.

A resilient organisation must ensure that its core business processes are robust and secure. Business continuity plans and procedures aim to achieve robust business processes, which in turn contribute to achieving resilient organisations. Business continuity planning is, therefore, an essential part of building organisational resilience. (BS 25999-1:2006, p.6)

In practice few organisations can claim to be robust or enjoy absolute security. By definition, a robust enterprise shoud be able to confront and overcome all threats at all times with little or no impact on its operational targets. Such a goal would be prohibitively costly for most organisations. A more realistic and achievable goal is organisational resilience.

General and specified resilience

An organisation may be designed and resourced to be resilient against a range of specified risks with known likelihood and impact. Examples of specified resilience would be the ability of a company such as Sydney Water to cope in the event of power outages, loss of data or industrial action. Existing management tools including risk management, business continuity and emergency planning can be used to build specified resilience.

General resilience refers to the ability of an organisation to cope against a range of threats where the likelihood, scale and impact of the events are unknown. Examples of general resilience would be the ability of Australia's farmers and cotton growers to adapt to climate change and accommodate market volatility. Emphasis needs to be placed on leadership, adaptability and a strong organisational ethos and values. Organisations with a strong ethos and values tend to be resilient; they have a firm and constant frame of reference which encourages staff and employees at all levels to remain committed to the vision and purpose of the organisation, even in times of crisis.

BUILDING ORGANISATIONAL RESILIENCE

Understanding the organisation and its environment

As discussed earlier in this paper, managers of resilient organisations should understand at board level the environment in which their organisations operate, and be aware of changes which may represent a risk to their people, facilities, activities, products, services and supply chains. Some of these changes are predictable such as the increasing global competition for raw materials and fossil fuels; some changes are probable such as increasing financial volatility and market regulation; other changes are possible such as the impact of natural disasters and terrorist acts.

Many of the changes will affect the organisation’s strategic and operational environment. By definition, an organisation does not control its external environment, but managers need to understand the increasingly complex cultural, political, legal, regulatory, technological, economic, natural and competitive context within which their organisation operates. They need to monitor the key issues and trends that may impact on the objectives of the organisation, and the perceptions and values of external stakeholders.

As changes occur to the external environment there is a need to constantly review the suitability of the organisation's vision, values, ethos and culture; the efficiency and contribution of its capabilities and assets including buildings, equipment, people, information and designs; the effectiveness of its procedures, activities and services; and the organisation's willingness to take risk. The Business Continuity Management Handbook (HB221: 2004) published by Standards Australia states that managers must formally “…. determine the business impact of the disruption of each critical business function …. and the maximum period of time before the loss (of a function) affects overall operations.”

Tools exist to assist managers determine critical activities and ascribe levels of performance and acceptable periods of disruption. IBM uses four levels to predict an organisation’s ability to withstand a potentially disruptive event to its information systems: platinum, gold, silver and bronze. The gold standard, for example, requires near continuous availability of 99.99 percent with service recovery of less than five minutes at a local level, and less than two hours for the data centre. (IBM Business Continuity and Resiliency Services, 2009)

Policy and planning

A resilient organisation requires commitment at board level to avoid, prevent and reduce the likelihood and consequences of disruptive events. This commitment should normally be in the form of a policy statement, the allocation of resources to build and maintain the organisation's ability to overcome disruptive events, and routine assessments of the organisation's business continuity procedures. Such statements provide a frame of reference which encourages everyone to remain committed to the vision and purpose of the organisation, even in times of disruption and crisis.

Organisations must establish and implement formal processes for identifying, analysing, evaluating and treating risk. Such risks will include intentional, unintentional and naturally-caused hazards and threats that have a potential to impact on the organisation's assets, operations and supply chain. There is no shortage of standards and guides on how to manage risk. Indeed, Charlette (2006) suggests the proliferation of risk standards may be counterproductive by diverting management attention from the full range and complexity of the risks facing their enterprise.

Conventional risk management, which has its roots in engineering and management science, can cope with predictable threats and quantifiable risks. In situations where the risk is considered to have potentially high impact and the likelihood is assessed to be very low or uncertain, it may be impossible or too costly to treat all such risks. Indeed, in such circumstances the acceptability of risk will often be shaped by judgement, which Gardner (2009) suggests is influenced by personal experiences, unjustifiable fear and bias, and is therefore unreliable. Concepts such as enterprise risk management attempt to overcome the shortcomings of conventional risk management by integrating the assessment and treatment of risk into the organisation's strategic and operational management processes, and thus ensure that risk is not considered in isolation.

Organisations should develop business continuity plans to address a range of potential threats. Business continuity has its roots in disaster recovery, which emerged in the 1960s as companies began to store backup copies of their critical data at alternate sites. By the mid 1990s, the concept expanded its scope and is now used to describe continuity across the entire enterprise, from facilities to people to communications. In 2006, the British Standards Institute published a national code of practice and specification for business continuity which has since been adopted by a number of countries as a *de facto* international standard.

International management consultancies such as KPMG have noted that some financial institutions are refocusing their efforts "…. beyond the traditional boundaries of business continuity, not only to survive crises stemming from (global risks) but to protect and potentially enhance shareholder value in the long term. Plans and procedures which define how critical business areas will continue to function during disruptive events are becoming more routine, more sophisticated and more connected." (KPMG, 2007, p.4)

Organisations are becoming increasingly cooperative in sharing information on potential threats and hazards. In Australia, the Trusted Information Sharing Network (TISN) provides a forum where the owners and operators of critical infrastructure such as financial institutions, water and energy providers can work together, sharing knowledge on common security issues. The TISN, which is promoted by the Attorney-General's Department aims to provide "…. a safe environment where industry and government can share vital information on critical infrastructure protection and organisational resilience. The TISN has established a truly collaborative relationship between business and government, based on trust, that is helping to build a more resilient Australia." (www.tisn.gov.au)

Notwithstanding such cooperative arrangements, it is important to recognise the competitiveness of commercial enterprises as they seek to maximise the value of their investments, contain "recovery workspace" costs and position themselves to seek commercial opportunities when disaster strikes. In some cases, organisations may not wish to invest as much as they should in building resilience, and thus expose themselves to excessive risk. For this reason we must expect increased regulation from governments to require organisations to increase their resilience by reducing and offsetting risks, and by enhancing business continuity plans and capabilities.

Implementation and operation

The international standard on societal resilience (ISO/PAS22399, 2009) and US standard (ANSI/ASIS SPC.1-2009) stress the importance of top management providing sufficient resources to establish, implement, maintain and improve organisational resilience. Resources includes information, management tools and financial support, and also people with specialist skills and knowledge. Both standards stress the importance of exercises and other means to test the appropriateness and efficacy of an organisation's plans, processes and procedures, including stakeholder relationships and infrastructure dependencies. Exercises should be designed and implemented in a manner that limits disruption to operations and exposes people, assets and information to minimum risk. They should be conducted regularly, or following significant changes to the organisation's mission and/or structure, and lessons learned should be formally recorded in a post-exercise report. Such reports should assess the appropriateness and effectiveness of the organisation's risk and business continuity plans, processes and procedures including non-conformities, and should propose corrective and preventative action.

Internal audits are also an essential management tool by assuring that organisations are meeting regulatory requirements, and where appropriate are consistent with international and national standards. The US Institute of Internal Auditors (2009, p.2) point out that ".... today’s governance arena requires boards of directors and their committees to be proactive, informed, investigative and accountable. Directors need to be realistic about their personal liability under local and national laws." Fiduciary duties – the obligations of care and loyalty - and the expectation that directors will act in good faith are particularly important in the event of a disaster, and audits aim to ensure that such duties are understood and are being applied.

Organisations need people who are competent through education, training and experience to develop and implement risk management and business continuity plans. In particular, organisations need staff and employees able to identify significant hazards, threats and risks, and potential impacts associated with their work, and can apply procedures to reduce the likelihood and manage the consequences of a disruptive event. In reality, few organisations will experience major disruptions and therefore experience can best be achieved through exercises and rehearsed drills. IBM (2007) and others stress that exercises should be conducted regularly, following changes to the organisation’s mission and/or structure or following significant changes to the operating environment. Exercises ensure that business continuity procedures remain relevant and confirm that staff are familiar with what is expected of them.

Although staff members may rally immediately after an event, resilience planning must take account of the psychological impact of a disaster, and such impact may not become evident for some time. KPMG, in their paper *Living on the Frontline: the Resilient Organisation* suggest that counselling may be required. “This is borne out by studies of individuals who were directly affected by 9/11. These revealed that in the medium term after the attack, three quarters of those surveyed experienced depression, nearly half had impaired concentration and a third developed insomnia. Significantly, (resilience planning) must be flexible enough to cope if a significant number of staff are either unable or unwilling to work in the aftermath of a disaster.” (KPMG, 2007, p.12)

Adaptability and flexibility

We live in a world that is constantly evolving through natural processes and in some cases by the intervention of mankind. There is common agreement in the resilience literature that systems, organisations and people who are able and willing to adapt to change tend to be more resilient.

General von Moltke, who was Chief of Staff of the Prussian Army in the 19th century is credited with the military principle that “no plan survives first contact with the enemy.” This principle is just as relevant for organisational resilience planning today as for military operations. Leaders and managers must be wary of adopting an ‘anchoring heuristic’ approach which Dan Gardner describes in his book *Risk: the Science of Politics and Fear* as the tendency of people to base decisions on familiar events, previous actions and rehearsed procedures (Gardner, 2008). When disaster strikes, continuity plans may need to be radically adapted to reflect new circumstances, or in some cases discarded to ensure that appropriate and considered action is taken.

Resilience thinking should encourage adaptability and flexibility. At the operational level, there may be a need to move resources or work prior to, during, or immediately following a disaster. At the strategic level, a major disruption may require a transformation of the organisation to a new business model with a new organisational structure.

Measuring resilience

There is a management maxim, attributed to Peter Druker that "…. if you can't measure it, you can't manage it." No matter how much is written on the principles of organisational resilience, or on the steps to be taken by managers to improve their understanding of risk, or the procedures to provide continuity, there is a need to measure current levels of resilience and to establish measurable objectives and targets for improved resilience.

In 1885, Robert Mallet developed a measure – the *modulus of resilience* – as a means of assessing the ability of materials to withstand severe conditions. The modulus still forms part of the design codes of civil and mechanical engineers. There has been considerably less progress in measuring the resilience of individuals, communities or organisations.

Recently, IBM (2009) proposed a *business resilience framework* which aims to assess the resilience of a complete organisation. The IBM model comprises 140 components, referred to as objects, which together can be used to model an organisation and its IT infrastructure. The objects are grouped on six levels, referred to as layers, and each object is given attributes which can be assessed in terms of risks and opportunities.

The IBM framework is a highly structured model which draws on the experience of earlier maturity models, in particular the Capability Maturity Model developed by Carnegie Mellon University in the late 1980s. The IBM framework is a comprehensive and adaptable tool for measuring organisational resilience, but its 140 objects require large amounts of data to be collected, collated and recorded. Collecting so much data would be expensive and therefore probably unattractive to many small and medium sized enterprises.

A simpler framework, such as the balanced scorecard, may be more attractive. The original *balanced scorecard* was developed in the 1990s by Robert Kaplan, an accounting professor at Harvard University and David Norton, a consultant from Boston. (Norton and Kaplan, 1996) The purpose of the original scorecard was to translate the vision and strategy of an organisation into just four groups of objectives, measures and targets, known as *perspectives*. Most scorecards use only four or five measures for each perspective, requiring no more than 20 indicators in total. Balanced scorecards continue to evolve and adapt to reflect the particular needs of communities of interest, such as government departments, non-governmental organisations, hospitals, schools and associations.

By themselves, tools such as the balanced scorecard and IBM's business resilience framework will not make organisations more resilient, but they should provide leaders with a clearer understanding of the key issues requiring further management effort and/or investment, including the organisation's supply chain partners.

EMBEDDED RESILIENCE

In our attempts to understand the concept of resilience, and to identify the fundamental characteristics which enable organisations to survive emergencies and crises, it is useful to consider examples of organisations routinely required to operate in hostile and uncertain environments. This section considers how two types of enterprise embed resilience into their structures, systems, leadership, ethos and culture: the military and NGOs operating in the humanitarian sector.

The military

The Armed Forces of Australia, like most professional defence forces, consider that organisational effectiveness – which is often referred to as *fighting power* by the military - is achieved by harnessing all of its intellectual, moral and physical resources. (LWD 1, 2008) This fundamental concept draws on the published works of great military thinkers such as Clausewitz (1780-1831), Fuller (1878-1966) and Liddell Hart (1895-1970. The intellectual component provides the knowledge to fight; the moral component provides the will to fight; and the physical component provides the means to fight. The role of commanders is to integrate these three components in a way that enables military units and formations to achieve their required objectives.

The *intellectual component* – which is sometimes referred to as the *conceptual component* – provides the intellectual basis and justification for the use of the military, and contributes the ideas and information needed for effective decision-making. It draws on experience, improvements to operational practice (gained through lessons learned, analysis and experimentation) and a thorough analysis of the immediate risks and future threats. The intellectual component provides commanders with the ability to understand the context within which they operate, and serves as the foundation upon which adaptability and innovation may be exercised, to enable success.

In the midst of chaos and uncertainty, individuals need to overcome fear and rise above their personal circumstances in the pursuit of organisational goals. The moral component is about getting people prepared, motivated and inspired to confront and overcome dangerous and difficult circumstances. British Defence Doctrine defines the *moral component* as a combination of moral cohesion, motivation and effective leadership. (JDP 0-01, 2008) Moral cohesion occurs when individuals want to work together and provide each other with support to achieve a common enterprise; it draws on shared experiences, a common sense of worth and an expressed collective identity, which is sustained by shared values and standards. It embodies genuine and deep comradeship that endures, notwithstanding violence and the fear of death and injury, and can best be described by the term *esprit de corps.* Motivation is a product of training, confidence in equipment and procedures, effective leadership and management, self-respect, mutual respect, and a clear understand-ing of what is going on and what is required. Motivation and high morale are interdependent.

The *physical component* of a military capability provides the means to fight. It includes people, equipment, collective performance and sustainability. Professional development ensures that individuals have the necessary skills, not just of their current appointment but to be able to carry out other tasks if the situation requires. Collective performance is characterised by high levels of cohesion, confidence and proficiency among military units and formations that have trained and operated together. The credibility and effectiveness of a military force rests upon its sustainability which is a combination of logistic support, infrastructure, communications and information management. Conversely, inadequate sustainability constrains the tempo of military operations.

There is remarkable similarity between the enduring principles of resilience which the military require of individuals and units, with the more general needs of organisational resilience. However, much of the literature on organisational resilience tends to be quite narrowly focused and often reflects particular interests and issues such as national security threats, the role of business management tools and standards, or intangibles such as leadership and organisational values. A more complete approach, embracing the intellectual, moral and physical components of organisational resilience is worthy of further study.

Non-governmental organisations

The concept of resilience is best known in the humanitarian and development sectors through the *Hyogo Framework of Action for 2005-2015* which aims to assist in building the resilience of nations and communities. (UN ISDR, 2005) The framework was the product of a major conference held in Hyogo, Japan in January 2005 involving UN organisations, donors and major international NGOs.

The Hyogo Framework has three strategic goals: (1) a more effective integration of disaster risk management into development policies, planning and programming; (2) the systematic use of risk reduction planning into preparedness, emergency response and recovery programs; and (3) the development of resilient institutions, mechanisms and capacities at all levels, in particular for communities at risk. For the purposes of this paper, however, the focus will be on international NGOs operating in the humanitarian sector rather than developing resilient national capabilities.

NGOs exist to bring about change in individuals and society by reducing suffering, providing aid and comfort, and fighting poverty and injustice. They are driven by a set of values and beliefs to achieve humanitarian goals, in contrast to commercial organisations which deliver products and services to achieve financial outcomes. By their very nature, many NGOs must operate in volatile, uncertain, complex, ambiguous and often highly dangerous situations. They have to cope in the face of adversity. To succeed they must be resilient.

Like the military, the effectiveness of NGOs is achieved by harnessing all their resources in a manner that suits the circumstances. No two missions are identical, and as such NGOs need to have plans which are adaptable and agile, procedures and funding that enables equipment and stores to be acquired rapidly, and staff who are driven to achieve outcomes even in times of crisis and hardship.

Successful NGOs place considerable emphasis on planning and preparation. Like the military, NGOs draw on experience, lessons learned, analysis and innovation. The operations rooms of organisations such as Oxfam, Medécin San Frontiers and World Vision work in much the same way as the operations rooms of the military or the emergency services. Considerable investment is made on collecting, collating, analysing and presenting information in a manner that helps decision-making. NGOs responding to major disasters face particular challenges in having to make rapid decisions, often based on incomplete or misleading information. Plans may need to be adapted or completely re-written, and thinking needs to be creative and agile in response to evolving situations.

One of the greatest challenges facing NGOs is the need to have the right equipment and stores in the right place at the right time. Most of the major NGOs have warehouses stocked with emergency supplies; for example Oxfam has pre-positioned stocks at depots around the world, and has prepared standing contracts to draw on cargo ships, aircraft and road transport to move equipment and stores at very short notice. Concepts such as just-in-time and lean logistics are usually inappropriate and are seen as being incompatible with the needs of NGOs operating in uncertain situations.

Successful organisations operating in the humanitarian sector place great emphasis on teamwork by encouraging cohesion, mutual respect, professional competence and a willingness to work in multicultural and multidisciplinary teams. Job descriptions place great emphasis on the commitment of employees to the aims and values of the organisation. Such emphasis is quite understandable as success is achieved through comradeship and a sense of common purpose that endures, regardless of personal hardship and adversity. Like the military, NGOs place considerable weight on moral cohesion, motivation and effective leadership.

Indeed there are many parallels between international NGOs and the military. In both cases, individuals consider their own needs to be subservient to those of their team, unit or organisation. Both need to build resilience at different levels of the organisation. To achieve such resilience they need effective leadership and vision, a strong ethos and moral values, a culture which encourages adaptability, the willingness to deal with uncertainty, and the ongoing improvement of procedures and practices. Indeed, the military assessment of operational effectiveness in terms of an organisation's moral, intellectual and physical capital is equally relevant to NGOs operating in situations which are fraught with complexity, uncertainty and danger.

CONCLUSIONS

As our society becomes more complex and interconnected, and the impact of global factors becomes more immediate and menacing, organisations will become more exposed to disruptive events from a broad range of threats and hazards.

This paper acknowledges the role of risk management in providing leaders and managers with greater understanding of the threats facing organisations and the options for mitigating the likelihood and severity of disruptive events. The paper also recognises the contribution of business continuity planning to build more robust organisational structures and procedures.

Organisational resilience is a new management concept. It does not replace risk management or business continuity planning. Indeed, organisational resilience is a goal, whereas risk management and continuity planning are management tools which can be used to achieve that goal.

Some critics argue the concept introduces an additional and unnecessary level of complexity, and further extends an already stretched management vocabulary. But the concept is already being applied to organisations in the private, public, not-for-profit and non-governmental sectors, and there is a growing consensus on its utility. A US standard on the requirements of organisational resilience has been translated into a number of languages, and recently has been accepted by the US, Danish and Dutch national standards bodies.

Lessons can be drawn from organisations which routinely operate in hostile and uncertain environments such as the military and NGOs working in disaster relief and post-conflict countries. Indeed, the military description of operational effectiveness in terms of a unit's moral, intellectual and physical capital is relevant to other types of organisation seeking to become more resilient.

This paper has argued that organisational resilience is a powerful and useful concept. There is still some confusion on how best to apply the concept in a reliable and consistent manner, and currently there are no universally agreed metrics for measuring resilience. The challenge facing us now is how best to develop and promote organisational resilience in Australia in a way that assists the Government develop policy and enables managers to build organisations which are able to operate more successfully and confidently in our increasingly volatile, uncertain, complex and ambiguous world.

Bibliography:

ASIS SPC.1-2009, Organizational Resilience Standard: security, preparedness and continuity management systems – requirements with guidance for use, American National Standards Institute, Inc.

Charlette, R.N. (2006) 'A risk of too many risk standards' *Sixteenth Annual International Symposium of the INCOSE.* 8 – 14 July2006.

Clausewitz, Carl Von (1874). *On War – Volume 1*. Edited and translated by Michael Howard and Peter Paret 1976, rev. 1984. Princeton: Princeton University Press.

Cork, S., Walker, B. and Buckley, R. (2008) *How Resilient is Australia*. Canberra: Australia21.

Cork, S., Walker, B. and Buckley, R. (2009) *Rapid and Surprising Change in Australia's Future*. Canberra: Australia21

Courtney, H., Kirkland, J. and Viguerie, P. (1997) 'Strategy under uncertainty'. *Harvard Business Review.* December 1997.

DCDC (2008) *Joint Doctrine Publication 0-01: British Defence Doctrine, Chapter 4 (Fighting Power*). Shrivenham: Defence Concepts and Doctrine Centre.

DFLWS (2008) Land Warfare Doctrine 1: *The Fundamentals of Land Warfare, Chapter 5 (Fighting Power).* Canberra: Defence Publishing.

Durodie, W. (2005) 'The limitations of risk management in dealing with disasters and building social resilience' *Tidsskriftet Politik,* Volume 8, Number 1, March 2005*,* pp.14-21

Drucker, P.F. (1954) *The Practice of Management.* New York: Harper and Row.

Drucker, P.F. (1990) *Managing the Non-profit Organization.* Oxford: Butterworth-Heinemann Ltd.

Economist Intelligence Unit (2007) *Business resilience: ensuring continuity in a volatile environment.* London: EIU.

Economist Intelligence Unit (2006) *Catastrophe risk management: preparing for potential storms ahead.* London: EIU.

Economist Intelligence Unit (2009) *Managing risk in perilous times: practical steps to accelerate recovery.* London: EIU.

Fuedi, F. and Roberts, S. (2004) *Disaster and contemporary consciousness: the changing cultural frame for the experience of adversity, Draft Report.* Downloaded from www.kent.ac.uk on 5 April 2010.

Gardner, D. (2009) *Risk: the science and politics of fear.* London: Virgin Books.

Government of Australia (2010) *Australia to 2050: future challenges (Intergenerational report).* Canberra: Attorney-General's Department.

Government of Australia (2010) *Adapting to Climate change in Australia: an Australian Government position paper.* Canberra: Department of Climate Change.

Hamel, G. and L. Välikangas (2003) 'The Quest for Resilience'. *Harvard Business Review.* September 2003.

IBM Business Continuity and Resilience Services (2008) *Five essential elements of business recovery.* New York: IBM Global Services

IBM Business Continuity and Resilience Services (January 2009) *Business resilience: The best defense is a good offense.* New York: IBM Global Services

IBM Business Continuity and Resilience Services (June 2009) *Beyond disaster recovery: becoming a resilient business.* New York: IBM Global Services

Institute of Internal Auditors (2009) 'A Global Perspective of Risk'. *Tone at the Top, Issue 43, May 2009.* Altamonte Springs: The Institute of Internal Auditors.

Kaplan, R.S. and Norton, D.P. (1996) *Translating strategy into action: the balanced scorecard*. Boston: Harvard Business School.

KPMG (2007) *Living on the front line: the resilient organisation.* Publication Number 306166 of March 2007. Downloaded from www.kpmg.com on 8 April 2010.

McAslan, A.R.R. *The Concept of Resilience: understanding its origins, meaning and utility*. Adelaide: Torrens Resilience Institute.

McClelland, R. (2009*) Remarks at the Critical Infrastructure Advisory Council Meeting.* 9 December 2009. Sydney

Marino, F. (2009) Organizational resilience for all. Miami Beach: Security Director LLC

NIAC (2009) *Critical infrastructure resilience: final report and recommendations*. 8 September 2009. Downloaded from www.dhs.gov on 8 April 2010.

Putnam, R. (1995) *Bowling Alone: America's Declining Social Capital,* Journal of Democracy 6:1, pp.65-78

Robb, D. (2000) 'Building Resilient Organizations' *OD Practitioner,* Volume 32, Number 3, 200*,* pp.27-32.

HB 221:2004 (2004) *Business Continuity Management Handbook.* Sydney: Standards Australia.

Steffen, W. (2009) *Climate Change 2009: Faster change and more serious risks*. Canberra: Australian Government Department of Climate Change.

United Nations (2009) *Report of the Commission of Experts of the President of the United Nations General Assembly on Reforms of the International Monetary and Financial System.* New York: United Nations.

UN ISDR (2005) *Hyogo Framework for Action 2005-2015: Building the resilience of Nations and Communities to Disasters,* Final report of the World Conference on Disaster Reduction (A/CONF.206/6), 18-22 January 2005, Kobe, Hyogo, Japan.

United Nations Population Fund (2009) *State of world population 2009.* New York: United Nations.

UK Cabinet Office (2003) *Draft Civil Contingencies Bill*. Norwich: HMSO.

World Economic Forum (2010) *Global Risks 2010: A Global Risk Network Report*. Geneva: World Economic Forum.