Chapter 5
Risk and Decision-Making for Extreme Events: Climate Change and Terrorism

Mark G. Stewart

Abstract Terrorism and climate change are extreme events that frighten and alarm. This makes decision-making for these hazards or threats all the more difficult, particularly when decision-makers are risk averse. This chapter will describe how risk-based approaches are well suited to optimising decisions related to these extreme events. Stochastic methods are used to model threat likelihood, vulnerability, effectiveness of protective strategies, exposure and costs. The concepts will be illustrated with current research of risk-based assessment of counterterrorism and climate adaptation strategies. The case studies consider (1) protection of new bridges against terrorist attack and (2) climate change and cost-effectiveness of designing new port facilities to be less vulnerable to severe corrosion.

5.1 Introduction

Cyclones, earthquakes, tsunamis and floods are natural hazards that cause significant loss of life and economic and social losses. Added to this are 'man-made' hazards such as climate change and terrorism. These hazards are low-probability—high-consequence—events which in recent times are more commonly referred to as 'extreme events'. Extreme events illicit extreme reactions—risk aversion, probability neglect, cost neglect, and worst-case thinking—that may distort the decision-making process in an effort by policymakers to be seen to be 'doing something' irrespective of the actual risks involved. Policymaking in these circumstances becomes a 'risky business' (Hardaker et al. 2009). If rational approaches to public policymaking are not utilised, then politically driven processes 'may lead to raising unnecessary fears, wasting scarce resources, or ignoring important problems' (Paté-Cornell 2002).

Terrorism and climate change are extreme events of much interest. They can engender fear in the community, and predictions of impending doom are often overstated. Many terrorism and climate change 'risk' and 'risk management' reports

M.G. Stewart (✉)
Centre for Infrastructure Performance and Reliability, The University of Newcastle, Newcastle, NSW 2308, Australia
e-mail: mark.stewart@newcastle.edu.au

P. Gardoni, J.M. LaFave (eds.), *Multi-hazard Approaches to Civil Infrastructure Engineering*, DOI 10.1007/978-3-319-29713-2_5

dwell on lists of vulnerabilities and consequences. There is seldom mention of probabilities, quantitative measures of vulnerability or the likelihood of losses. While useful for initial risk screening, intuitive and judgement-based risk assessments are of limited utility to complex decision-making since there are often a number of climate or threat scenarios, adaptation or counterterrorism options, limited funds and doubts about the cost-effectiveness of protective measures. In this case, the decision-maker may still be uncertain about the best course of action. For this reason, there is a need for sound system and probabilistic modelling that integrates the performance of infrastructure systems with the latest developments in stochastic modelling, structural reliability and decision theory.

There is increasing research that takes into account the changing climate risks and life cycle costs in engineering to reduce the vulnerability or increase the resiliency of infrastructure—we refer to this as 'climate adaptation engineering'. Climate adaptation engineering is defined as measures taken to reduce the vulnerability or increase the resiliency of built infrastructure to a changing climate; this may include, for example, enhancement of design standards (higher design loads or flood levels), retrofitting or strengthening of existing structures, utilisation of new materials and changes to inspection and maintenance regimes (Stewart et al. 2014; Stewart and Deng 2015). The IPCC (2012) reports that 'vulnerability is a key factor in disaster losses, yet it is not well accounted for'. Probabilistic terrorism risk assessment methods have been developed to assess the risks of terrorism and effectiveness of risk-reducing measures (Mueller and Stewart 2011a, b, 2016). While the jargon differs, the decision support approaches to counterterrorism and climate adaptation measures have much in common, as do the challenges. The chapter aims to draw out these issues in more detail.

This chapter will describe how risk-based approaches are well suited to optimising decisions related to extreme events, in this case, climate adaptation strategies and counterterrorism measures. An important aspect is assessing when protective measures become economically viable, if protection can be deferred, and decision preferences for future costs and benefits (many of them intergenerational). Stochastic methods are used to model threat likelihood, vulnerability, effectiveness of protective strategies, exposure and costs. The concepts will be illustrated with current research of risk-based assessment of counterterrorism and climate adaptation strategies. The case studies consider (1) protection of new bridges against terrorist attack and (2) climate change and cost-effectiveness of designing new port facilities to be less vulnerable to severe corrosion caused by an increase in seawater temperature.

5.2 Key Issues

There are a number of issues and questions related to controversial and emotive issues such as terrorism, climate change and other extreme events. These contribute to risk aversion and are discussed as follows.

5.2.1 Worst-Case Thinking

Worst-case thinking, or hyperbole, tends to dominate the thinking of many climate change and terrorism experts. In 2008, Department of Homeland Security (DHS) Secretary Michael Chertoff proclaimed the 'struggle' against terrorism to be a 'significant existential' one (Mueller and Stewart 2011a). And in 2014, Mayor Bill de Blasio of New York at a UN summit proclaimed that 'We know humanity is facing an existential threat' from climate change (Grynbaum 2014). The notion that a threat short of all-out nuclear war could be existential to humanity is hard to fathom. If business-as-usual predictions are biased towards impending doom, then this justifies any response no matter the cost in loss of civil liberties, quality of life and treasure.

5.2.2 Cost Neglect

While it is not difficult to list threats and vulnerabilities, what is more challenging is to ascertain the cost to reduce these threats and vulnerabilities and to decide who pays and when. There is a notion that safety is infinitely good, and no cost is too high. There is no attempt to compare costs against benefits.

5.2.3 Probability Neglect

Many analysts base their findings on threats or scenarios that they assume will occur. There is no consideration of the likelihood of a terrorist attack, that a specific CO_2 emission scenario will occur or that adaptation will be effective. For example, a US 2014 climate risk assessment report predicts trillions in dollars of damage due to climate change for the business-as-usual scenario—i.e. the USA continues in its current path (Risky Business 2014). There is no attempt to quantify the likelihood that CO_2 emissions will continue unabated for the next 85 years, that CO_2 mitigation measures will be implemented, that adaptation measures are implemented, or of the impact of improved or game-changing technologies. Sunstein (2003) terms this as 'probability neglect' that 'people's attention is focused on the bad outcome itself, and they are inattentive to the fact that it is unlikely to occur'. There is no certainty with predictions, nicely summed up by physicist Niels Bohr: 'Prediction is very difficult, especially if it's about the future'.

5.2.4 Opportunity Costs

Policymakers that act before they carefully consider the implications of their actions can result in undesirable outcomes which are often referred to as 'opportunity

costs'. For example, increased delays and added costs at US airports due to new security procedures provide incentive for many short-haul passengers to drive to their destination rather than flying, and, since driving is far riskier than air travel, the extra automobile traffic generated has been estimated to result in 500 or more extra road fatalities per year (Blalock et al. 2007). Using a DHS-mandated value of statistical life of $7.5 million (Robinson et al. 2010), this equates to a loss of $3.75 billion per year or nearly $50 billion over the period 2002–2014. A CO_2 mitigation strategy that reduces economic growth, particularly in developing countries, may reduce their ability to adapt. Weather- and climate-related fatality rates and economic losses are also 3–10 times higher in developing countries (IPCC 2012). Clearly then, if people are wealthier in the future, their well-being will be higher (Goklany 2008).

5.2.5 Acceptable Risk

The notion of acceptable risk is rarely raised in public discussions. The world is not risk-free. The generally accepted level of annual fatality risk (AFR) is one in a million (e.g. Stewart and Melchers 1997); see, for example, Murphy and Gardoni (2008) and Gardoni and Murphy (2014) for a fuller discussion on risk acceptability. The probability that an American will be killed by a terrorist in the USA, with the events of 2001 included in the count, stands at about one in four million per year (Mueller and Stewart 2016), or the probability an airline passenger will be killed by a terrorist act is a low one in 90 million per year (Mueller and Stewart 2016). By comparison, an American's chance of being killed in an automobile crash is about one in 8000, the chance of becoming a victim of homicide is about one in 22,000, and the chance of being killed by lightning is one in seven million per year. How much should we be willing to reduce a risk that is already very low, and is the risk reduction worth the cost?

5.3 Risk-Based Decision Support

Decision criteria for extreme events are typically based on (1) AFR and (2) cost-effectiveness of protective measures. Risk for a system exposed to a threat is

$$E(L) = \sum \Pr(T) \Pr\left(H\middle|T\right) \Pr\left(D\middle|H\right) \Pr\left(L\middle|D\right) L \tag{5.1}$$

where $\Pr(T)$ is the annual probability that a specific threat will occur (a terrorist attack, an emission scenario), $\Pr(H|T)$ is the annual probability of a hazard (wind, heat, explosion) conditional on the threat, $\Pr(D|H)$ is the probability of damage

or other undesired effects conditional on the hazard (also known as vulnerability or fragility) for the baseline case of no extra protection (i.e. 'business as usual'), $\Pr(L|D)$ is the conditional probability of a loss (economic loss, loss of life, etc.) given occurrence of the damage (resilience) and L is the loss or consequence if full damage occurs. In some cases, 'damage' may equate to 'loss' and so a vulnerability function may be expressed as $\Pr(L|H)$ which is equal to the product $\Pr(D|H)\Pr(L|D)$. The summation sign in Eq. (5.1) refers to the number of possible threats, hazards, damage levels and losses. If the loss refers to a monetary loss, then $E(L)$ represents an economic risk.

If the loss refers to fatalities, then $E(L)$ represents an AFR. Stewart and Melchers (1997) and Mueller and Stewart (2011a) reviewed the quantitative safety goals used by the US Nuclear Regulatory Commission, UK Health and Safety Executive, Australian and European hazardous industrial development regulators, US environmental carcinogenic exposure regulators and others. These government regulators are concerned with low-probability—high-consequence—failures. The consensus risk acceptance criteria obtained for involuntary fatality risk to an individual are:

- AFRs higher than 1×10^{-3}–1×10^{-4} are deemed unacceptably high.
- AFRs in the range of 1×10^{-4}–1×10^{-6} are generally tolerable if the benefits outweigh the risks to provide an economic or social justification of the risk.
- AFRs smaller than 1×10^{-6} are deemed as negligible and further regulation is not warranted. Risk is broadly acceptable (or tolerable) as long as precautions are maintained, and further improvements are not required if these involve high costs.

If we modify Eq. (5.1) where ΔR is the reduction in risk caused by protective measures (e.g. climate adaptation or counterterrorism), then expected loss after protection is

$$E_{\text{protect}}(L) = \sum (1 - \Delta R)\, E(L) - \Delta B \tag{5.2}$$

where ΔR is the reduction in risk caused by the protective measure, $E(L)$ is the 'business-as-usual' expected loss (risk) given by Eq. (5.1) and ΔB is the co-benefit such as reduced losses to other hazards, increased energy efficiency of new materials, etc. If there is an opportunity cost associated with a new measure, then ΔB becomes a negative value. Protective measures should result in risk reduction (ΔR) that may arise from a combination of reduced likelihood of the hazard, damage states, safety hazards and people exposed to the safety hazard.

The challenging aspect of risk-based decision theory is predicting values of $\Pr(T)$, $\Pr(H|T)$, $\Pr(D|H)$, $\Pr(L|D)$ and ΔR. This information may be inferred from expert opinions, scenario analysis and statistical analysis of prior performance data, as well as system and reliability modelling. Since there is uncertainty associated with such predictions, the use of probability distributions to describe mean, variance and distribution type is recommended.

If the AFR lies in the generally tolerable region (e.g. 1×10^{-4} to 1×10^{-6}), then three criteria may be used to assess if the benefits of protective measures exceed their cost:

1. Net present value (NPV)
2. Probability of cost-effectiveness or Pr(NPV > 0)
3. Benefit-to-cost ratio (BCR)

The 'benefit' of a protective measure is the reduction in damages or losses associated with the protective strategy, and the 'cost' is the cost of the protective strategy. The net benefit or NPV is equal to benefit minus the cost. The decision problem is to maximise the NPV

$$\text{NPV} = \sum E(L)\Delta R + \Delta B - C_{\text{protect}} \tag{5.3}$$

where C_{protect} is the protection cost including opportunity costs that reduces risk by ΔR. Figure 5.1 shows how protective costs increase with risk reduction, while benefits increase. The optimal protection occurs when the NPV is a maximum, leading to optimal risk reduction. Relevant is what level of expenditure and risk reduction gives the greatest benefit and when does the law of diminishing returns kick in. The first dollars spent on protective measures are likely to be worthwhile, even if the last is not.

The BCR is

$$\text{BCR} = \frac{\sum E(L)\Delta R + \Delta B}{C_{\text{protect}}} \tag{5.4}$$

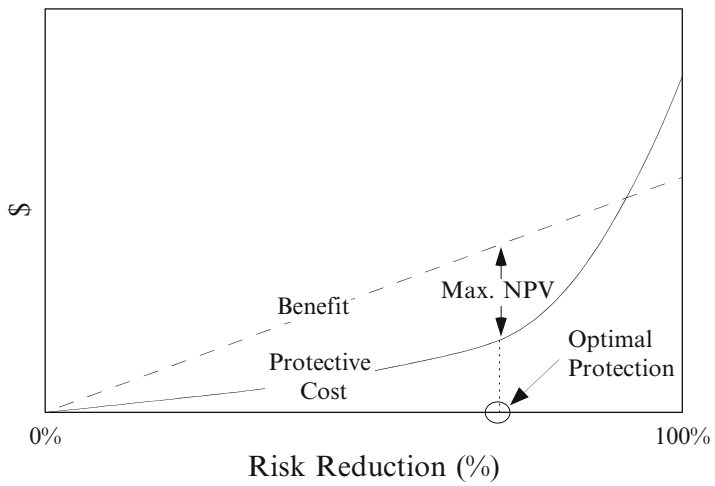

Fig. 5.1 Schematic of the NPV showing optimal protection

If parameters $\Pr(T)$, $\Pr(H|T)$, $\Pr(D|H)$, $\Pr(L|D)$ L, ΔR, ΔB and/or C_{protect} are random variables, then the output of the analysis (NPV or BCR) is also variable. This allows confidence bounds of the NPV or BCR to be calculated, as well as the probability that an adaptation measure is cost-effective denoted herein as $\Pr(\text{NPV} > 0)$. If the $\text{NPV} > 0$ or $\text{BCR} > 1$, then there is a net benefit and so the protective measure is cost-effective. Other notations and formulae can be used to provide optimal protection, but ultimately these also mostly rely on maximising the NPV.

If the probability that a specific threat will occur or $\Pr(T)$ is too unreliable, then a decision analysis based on scenario analysis where threat probability is decoupled from Eq. (5.1) provides an alternative decision-making criteria based on expected costs. The above equations can be generalised for any time period, discounting of future costs and more detailed time-dependent cost and damage consequences.

Threat, vulnerability, loss and protective costs are subject to considerable uncertainty due to lack of available data and models. For this reason, calculations of risks, costs and benefits will be imprecise. Hence, a 'breakeven' analysis may be useful where minimum threat probability, minimum risk reduction or maximum protective cost necessary for protective measures to be cost-effective is selected such that there is 50 % probability that benefits equal cost—i.e. $\text{mean}(\text{NPV}) = 0$. For example, if the actual cost of protection exceeds the predicted breakeven value, then protection is not cost-effective. Decision-makers can then judge whether a protective strategy meets these breakeven values.

Governments and their regulatory agencies normally exhibit risk-neutral attitudes in their decision-making as described by Eqs. (5.3) and (5.4) above. This is confirmed by the US Office of Management and Budget (OMB) which specifically states that 'the standard criterion for deciding whether a government program can be justified on economic principles is NPV—the discounted monetized value of expected net benefits (i.e. benefits minus costs)'—and that 'expected values (an unbiased estimate) is the appropriate estimate for use' (OMB 1992). This entails using mean or average estimates for risk and cost-benefit calculations and not worst-case or pessimistic estimates. Probability neglect is a form of risk aversion as decision-makers are clearly averse to events of large magnitude irrespective of the probability of it actually occurring. Utility theory can be used if the decision-maker wishes to explicitly factor risk aversion or proneness into the decision process (e.g. Stewart et al. 2011).

It is important to note that the issue of risk aversion is not a new one, but has been well researched and documented for politically sensitive and controversial decisions associated with nuclear power safety, aviation safety, pharmaceutical benefits scheme, environmental pollution and other extreme events. In these cases, risk acceptance criteria have been developed based on AFRs and net benefit analysis using expected (mean) values. In principle, decisions related to terrorism, climate change and other extreme events should be made with similar risk-based methodologies.

5.4 Terrorism Case Study: Design of New Bridges Against Terrorist Attack

Highway bridges are often seen as an attractive target for terrorists. There are 600,000 highway bridges in the USA and bridges seem to be especially vulnerable. As Chairman Bennie Thompson of the House of Representatives' Committee on Homeland Security insists, 'The U.S. highway system is particularly vulnerable to potential terrorist attacks because of its openness—vehicles and their operators can move freely and with almost no restrictions, and some bridge and tunnel elements are easily accessible and located in isolated areas making them more challenging to secure' (GAO 2009). However, a bridge is very difficult to damage severely because its concrete and steel construction already makes it something of a hardened structure. Building facades (glass, masonry, cladding) are far more vulnerable (Norville et al. 1999). The Global Terrorism Database shows that of the 14 bridges attacked by insurgents in the war zones of Iraq and Afghanistan between 1998 and 2007, the total number of fatalities was relatively few at 59, and no more than 10 were killed in any single attack.

The preferred method of attack is improvised explosive devices (IEDs). An IED is relatively simple to design and manufacture if done by well-trained personnel, resulting in reliabilities in excess of 90 % (Grant and Stewart 2012). However, the probability of an IED creating a damaging effect (damage in excess of $1 million or attack resulting in casualties) reduces to 23 % for terrorists in Western countries where there is less opportunity for IED operational skills to be acquired (Grant and Stewart 2015). In the USA this figure drops to 15 %. This was clearly evident from the second attack on the London Underground on 21 July 2005 where four IEDs failed to initiate and in Glasgow International Airport in 2007 and Times Square in 2010 where vehicle-borne improvised explosive devices (VBIEDs) failed to initiate. The probability of successful attacks using IEDs increases to 65 % for terrorists or insurgents in the Middle East (Grant and Stewart 2012).

An explosive blast will not blow up a bridge, but will more likely damage and weaken supporting elements, causing only partial collapse. Even if a bridge collapses, however, not all vehicle occupants on it will be killed. For example, the collapse of the ten-lane, 14-span, 580 m I35W bridge in Minneapolis in 2007 killed 13 people, but 111 vehicles were on the bridge at the time of collapse (NTSB 2008). A bridge collapse over the Arkansas River in 2002 killed 14 people when 11 vehicles, of the many that were on the bridge, plunged into the river (Bai et al. 2006). The unexpectedly high survival rates arise not only because the bridge only partially collapses but also because a car is designed to crumple on impact and thus absorb energy.

The replacement cost for a typical interstate highway bridge is set at $20 million. In addition to the economic cost of traffic diversion, there are other social and economic costs to a community. These are harder to quantify but may be in the order of tens to hundreds of millions of dollars because, although the loss of one bridge will not isolate a community, it will generally cause considerable inconvenience and

disruption. It is assumed that the replacement cost and social and economic costs to the community sum to $100 million. The expected number of fatalities is assumed as 20, at a cost of $150 million based on the value of statistical life of $7.5 million (Robinson et al. 2010). The total losses for a damaged bridge including both the loss of life and economic considerations is $L = \$250$ million.

Measures to enhance security for new bridges typically focus on strengthening columns and girders, additional steel reinforcement, minimum dimensions, adding lateral bracing and increasing standoff by bollards, security fences and vehicle barriers. Although there is much information available about design and retrofitting bridges to mitigate the effects of blast damage, there is little information about their cost. It is assumed that substantial mitigation of blast effects can be achieved for a new bridge at a cost of 5 % of a bridge's replacement value. If the bridge replacement value is $20 million, the cost of enhancing its design is then $1 million. Annualised over a design life of 75 years at 4 % and 7 %, discount rates result in security costs of $44,000 and $70,000, respectively. A middle value for strengthening results in a security cost of $C_{\text{protect}} = \$50{,}000$ per year.

It is generously assumed that protective measures reduce the risk by $\Delta R = 95\,\%$. We also include in these calculations that hazard likelihood (IED or VBIED detonating and causing a damaging effect) is rounded up to $\Pr(H|T) = 20\,\%$ as obtained from the GTD (Grant and Stewart 2015). It is then assumed there is 50 % likelihood that the VBIED will completely destroy the bridge killing 20 people ($\Pr(L|H) = 50\,\%$).

Table 5.1 shows the breakeven annual threat (attack) probabilities $\Pr(T)$ required at a minimum for security expenditures on protecting a bridge to be cost-effective. This breakeven analysis shows that protective measures that cost $50,000 per year and that successfully protect against an attack that would otherwise inflict $250 million in damage would be cost-effective only if the probability of a successful terrorist attack without them exceeds 0.2 % or one in 500 per bridge per year. If we assume risk is reduced only by 50 %, the minimum attack probability per year required for bridge protective measures to be considered cost-effective increases to 0.4 % per bridge. If the average cost of construction is halved to only $10 million per bridge, then C_{protect} is halved to $25,000, but if losses remain at $250 million, then Table 5.1 shows that the annual attack probability needs to exceed 0.1 % per bridge per year for counterterrorism protective measures to be cost-effective.

As a conservative estimate, it is now assumed in these calculations that bridges are 100 % vulnerable to attack—i.e. a VBIED will always detonate ($\Pr(H|T) = 100\,\%$), then destroying the bridge every time and always killing 20 people ($\Pr(L|H) = 100\,\%$). This is unlikely to be the case since there is not 100 % surety that an IED will initiate successfully, and that the blast will then cause bridge collapse and maximum consequences. In other words, the calculations assume that every attack will achieve 100 % success. In this unrealistic case, the breakeven attack probabilities shown in Table 5.1 will decrease tenfold. The evidence to date suggests that such a high attack probability is not being observed.

On the other hand, the co-benefit of counterterrorism protective measures may be considerable if strengthening a bridge to be more blast resistant has the co-benefit

Table 5.1 Probability of an otherwise successful terrorist attack, in percentage per year, required for protective security expenditures to be cost-effective, assuming the expenditures reduce the risk by 95 %

Cost of protective measures $C_{protect}$ (per year)	Losses from a successful terrorist attack (L)					
	\$100 million	\$250 million	\$1 billion	\$2 billion	\$10 billion	\$100 billion
\$25,000	0.3	0.1	0.03	0.01	0.00	0.00
\$50,000	0.5	0.2	0.05	0.03	0.01	0.00
\$100,000	1.1	0.4	0.11	0.05	0.01	0.00
\$250,000	2.6	1.1	0.26	0.13	0.03	0.00
\$500,000	5.3	2.1	0.53	0.26	0.05	0.01
\$1 million	10.5	4.2	1.1	0.53	0.11	0.01
\$5 million	52.6	21.1	5.3	2.6	0.53	0.05
\$10 million	105.3	42.1	10.5	5.3	1.1	0.11
\$100 million	1052.6	421.1	105.3	52.6	10.5	1.1

Note: Probability of 100 % denotes one attack per bridge per year

of reducing the risks from seismic, flood or other hazards. In this case, breakeven attack probabilities would reduce.

If there were one attack on a highway bridge every year in the USA, the attack probability would be only one in 600,000 per bridge per year (0.0002 %) because there are 600,000 bridges in the country. This probability is nowhere near the one in 500 likelihood of a successful attack required for bridge protective measures to be cost-effective. If the attack probability is a high 0.01 % per bridge per year then the BCR is only 0.05—i.e. \$1 of cost buys only 5 cents of benefits. In fact, the only threat against a US highway bridge in the USA since 9/11 was a terrorist plot to target the four-lane Brecksville-Northfield High Level Bridge near Cleveland, Ohio, in 2012.

If $\Pr(T)$ is taken as one in 600,000 or 0.0002 % per bridge per year, $\Pr(H|T) = 20\,\%$ and $\Pr(L|H) = 50\,\%$, the AFR (without protective measures) is 1.7×10^{-7} fatalities per year. This is less than the risk acceptance criteria of 1×10^{-6} fatalities per year, and so further protection is not warranted.

If there is a specific threat such that the likelihood of attack is massively increasing or if a bridge is deemed an iconic structure such that its perceived value is massively inflated, bridge protective measures may begin to become cost-effective. Thus, San Francisco's Golden Gate Bridge or New York's Brooklyn Bridge might be a more tempting target for terrorists than a more typical highway bridge.

Finally, it may seem prudent to provide counterterrorism protective measures for new bridges as the additional cost for a single new bridge may seem modest at approximately \$50,000 per bridge per year or a 5 % increase in construction costs and higher costs to retrofit existing bridges. The ASCE 2013 Infrastructure Report Card recommends that \$20.5 billion is needed annually to replace or repair existing bridges in the USA (ASCE 2013). Up to an additional \$2 billion per year in funding

would then be needed to provide counterterrorism protective measures for these new bridges. This is a significant sum of money and could be better spent elsewhere if the aim is to reduce risk and save lives, such as flood levee banks, tornado shelters or other infrastructure to reduce risks from natural hazards. See Mueller and Stewart (2011a) and Stewart and Mueller (2014c) for further details.

For assessments of risks, costs and benefits of building and airport protection, aviation security and policing, see Stewart and Mueller (2011, 2013, 2014a, b) and Mueller and Stewart (2011a, 2014, 2016).

5.5 Climate Adaptation Case Study: Deterioration of Port Infrastructure

The 2014 Intergovernmental Panel on Climate Change Fifth Assessment (AR5) Synthesis Report concluded that the 'Warming of the climate system is unequivocal, and since the 1950s, many of the observed changes are unprecedented over decades to millennia. The atmosphere and ocean have warmed, the amounts of snow and ice have diminished, sea level has risen, and the concentrations of greenhouse gases have increased'. What is less certain is the impact that rising temperatures will have on rainfall, wind patterns, sea level rise and other phenomena.

Steel sheet piling is commonly used in many ports and harbours worldwide. However, corrosion of steel sheet piling can result in metal loss and reduced structural capacity, which can then lead to failure (see Fig. 5.2). Corrosion results from a chemical reaction, so an increase in seawater temperature can accelerate the corrosion process. The Fourth Assessment Report of the Intergovernmental Panel

Fig. 5.2 Example of failure of a sheet pile retaining wall (photo courtesy of R Jeffrey)

on Climate Change predicts that average seawater surface temperature is 'likely' to increase by 6 °C over the next 100 years (IPCC 2007).

The corrosion of concern for this type of coastal infrastructure is a phenomenon known as accelerated low water corrosion (ALWC) (Melchers and Jeffrey 2013). The vulnerability $\Pr(D|H)$ of sheet piling to ALWC is obtained from a time-dependent structural reliability analysis. It is assumed, as is reasonable in practice, that the piles are unprotected, having no protective paint coatings or cathodic protection. Damage to the retaining wall will halt all dock works and associated services. Damage is defined as excessive deformation of the wall such as by visually noticeable deformation of pavements and dock areas.

Current design practice results in the installation of AU 25 U-profile sheet piles. However, if corrosion loss is expected to accelerate due to a changing climate, then a climate adaptation measure may be to select a stronger sheet pile with a larger thickness. In this case, an AU 26 sheet pile is 0.3–0.5 mm thicker and 3 % stronger than the AU 25 sheet pile.

The structural reliability analysis includes the stochastic variability of loads, soil properties, steel material properties, dimensions and corrosion processes. The vulnerability $\Pr(D|H)$ for the existing AU 25 and proposed AU 26 sheet piles allowing for a 6 °C seawater temperature increase over the next 100 years is shown in Fig. 5.3. The risk reduction arising from using the higher-capacity AU 26 steel pile is shown in Fig. 5.4. Clearly, even though the adaptation measure is the installation of slightly larger (3 %) piles, the risk reduction reaches 20 % early in the service life of the sheet piles.

It can be assumed that damage shown in Fig. 5.2 will lead to 100 % likelihood of loss, hence, $\Pr(L|D) = 100\,\%$. The economic loss (L) from damage of sheet piling can be considerable. The cost to repair damage is likely to be at least $1 million,

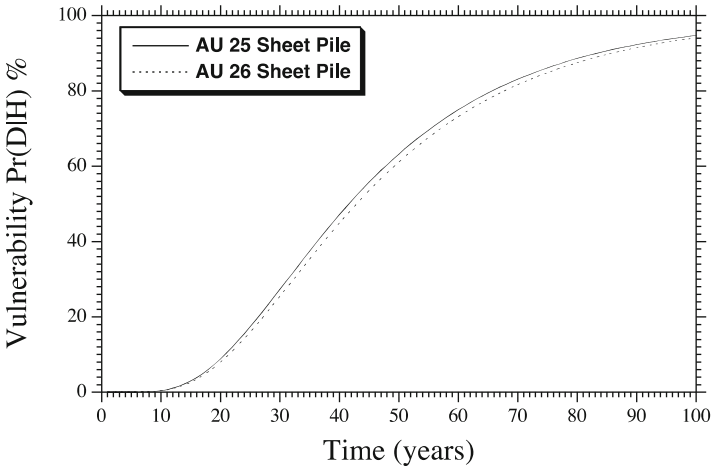

Fig. 5.3 Time-dependent vulnerability for sheet piles

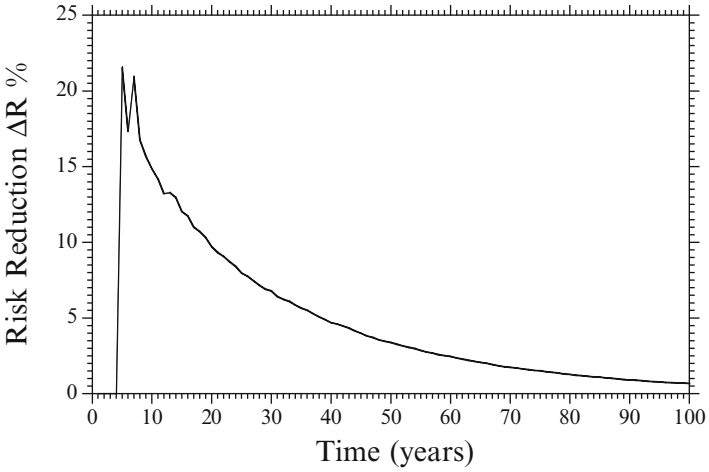

Fig. 5.4 Risk reduction from adaptation

and repair time is at least one month. To assess the indirect loss to the owner of a port, the economics of the Port Botany container terminal in Sydney is used as an illustrative example. The economic activity of the 12 shipping container berths runs to over $2 billion per year (Sydney Ports 2008). This includes costs to the asset owner, trucking costs, worker wages and economic gains from the efficient import and export of goods in Australia. If one of these 12 berths is unavailable due to sheet piling damage, then shipping may be diverted to other berths. However, if all berths are busy, then delays can be expected at a pro-rata cost of $14 million for loss of one berth for one month. An upper bound of economic loss, when also considering direct repair costs, is $15 million. A lower bound is $1 million assuming loss of one berth for one month does not disrupt normal shipping. A mid-estimate of $L = \$8$ million is thus reasonable.

The adaptation cost (C_{protect}) is based on the additional cost of purchasing larger AU 26 sheet piles. The AU 26 sheet piles are 2.5 % heavier than AU 25 piles. The additional material cost for a 200 m-long dock using 30 m-deep piles is approximately $10,000.

The existing present value risk calculated from Eq. (5.1) for a scenario-based analysis ($\Pr(T) = \Pr(H|T) = 100\,\%$) of a 6 °C increase in seawater temperature in 100 years and 7 % discount rate is $E(L) = \$745{,}830$. The average risk reduction over 100 years is 5.4 %. Assuming no co-benefits, the NPV (or net benefit) of this adaptation measure is NPV = $30,500. The benefit-to-cost ratio is BCR = 4.05. The use of larger AU 26 sheet piles is cost-effective for this climate scenario. This adaptation measure remains cost-effective even if adaptation costs double or economic losses are halved. The NPV will increase for discount rates lower than 7 %. Figure 5.5 shows the NPV as a function of time. The payback period (when benefit exceeds cost) is only 12 years.

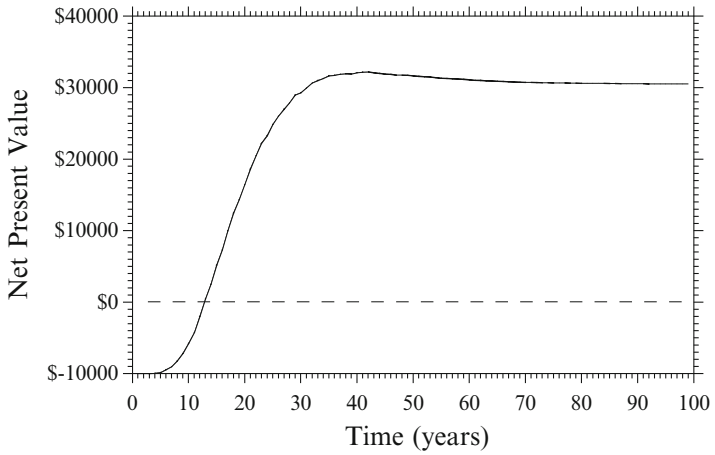

Fig. 5.5 Net present value for adaptation

This illustrative example shows that an adaptation measure that is low cost with a low risk reduction can still be cost-effective, particularly if the losses from infrastructure damage are relatively high. In other words, modest (or small) reductions in infrastructure vulnerability can be very cost-effective.

Finally, there is no certainty that existing design and construction practices are optimal. Design standards often are based on past experience, as well as new knowledge. However, they are seldom subject to a cost-benefit analysis due to modelling complexity and, more often than not, scarce resources to undertake work of this nature. Hence, it is desirable to assess the costs and benefits of existing designs. Moreover, there is likely to be uncertainty about climate scenarios. As such, it is useful to conduct a risk-based cost-benefit assessment for infrastructure assuming the current climatic conditions. The analysis reveals that for no change in seawater temperature, the NPV is $24,900. Hence, even if there is no change in seawater temperature, it is cost-effective to increase the size of sheet piling, in the present case, to AU 26. Hence, even if climate projections are overly conservative, adaptation measures still satisfies a 'no regrets' or 'win-win' policy (Susskind 2010).

Other case studies consider climate change and cost-effectiveness of designing new houses in Australia to be less vulnerable to severe storms (Stewart et al. 2014; Stewart 2014). To be sure, there are other case studies of assessing the efficiency and cost-effectiveness of climate adaptation strategies for built infrastructure, for example, floods and sea level rise (e.g. Hinkel et al. 2010; Hall et al. 2012; Botzen et al. 2013; Kundzewicz et al. 2013; Holden et al. 2013; Val et al. 2013), cyclones and severe storms (Bjarnadottir et al. 2011, 2013, 2014; Nishijima et al. 2012) and corrosion-reinforced concrete (Stewart and Peng 2010; Peng and Stewart 2014; Bastidas-Arteaga and Stewart 2015, 2016). For a general review, see Stewart et al. (2014).

5.6 Conclusions

Terrorism and climate change are extreme events that engender fear and anxiety in the community. Policymakers are also susceptible to these emotions. Risk-based approaches are suitable to assess the acceptability of risks and the cost-effectiveness of measures to reduce terrorism and climate impact risks. The concepts were illustrated with state-of-the-art applications of risk-based assessment for (1) the protection of new bridges against terrorist attack and (2) climate change and cost-effectiveness of designing new port facilities to be less vulnerable to severe corrosion caused by an increase in seawater temperature.

Acknowledgements The author thanks Dr Lizhengli Peng for generating the data for Fig. 5.3. The author also appreciates the financial support of the Australian Research Council and the Commonwealth Scientific and Industrial Research Organisation (CSIRO) Flagship Cluster Fund through the project Climate Adaptation Engineering for Extreme Events in collaboration with the Sustainable Cities and Coasts Theme, the CSIRO Climate Adaptation Flagship.

References

ASCE. (2013, March). *2013 Infrastructure Report Card*. Reston, VA: American Society of Civil Engineers.

Bai, Y., Burkett, W., & Nash, P. (2006). Lessons learnt from the emergency bridge replacement project. *Journal of Construction Engineering and Management, 132*(4), 338–344.

Bastidas-Arteaga, E., & Stewart, M. G. (2015). Damage risks and economic assessment of climate adaptation strategies for design of new concrete structures subject to chloride-induced corrosion. *Structural Safety, 52*(A, January), 40–53.

Bastidas-Arteaga, E., & Stewart, M. G. (2016). Economic assessment of climate adaptation strategies for existing RC structures subjected to chloride-induced corrosion. *Structure and Infrastructure Engineering, 12*(4), 432–449.

Bjarnadottir, S., Li, Y., & Stewart, M. G. (2011). A probabilistic-based framework for impact and adaptation assessment of climate change on hurricane damage risks and costs. *Structural Safety, 33*(3), 173–185.

Bjarnadottir, S., Li, Y., & Stewart, M. G. (2013). Hurricane risk assessment of power distribution poles considering impacts of a changing climate. *Journal of Infrastructure Systems, 19*(1), 12–24.

Bjarnadottir, S., Li, Y., & Stewart, M. G. (2014). Risk-based economic assessment of mitigation strategies for power distribution poles subjected to hurricanes. *Structure and Infrastructure Engineering, 10*(6), 740–752.

Blalock, G., Kadiyali, V., & Simon, D. H. (2007, November). The impact of post-9/11 airport security measures on the demand for air travel. *Journal of Law and Economics*, *50*(4), 731–755.

Botzen, W. J. W., Alerts, J. C. J. H., & van den Bergh, J. C. J. M. (2013). Individual preferences for reducing flood risk to near zero through elevation. *Mitigation and Adaptation Strategies for Global Change, 18*(2), 229–244.

GAO. (2009, January). *Federal efforts to strengthen security should be better coordinated and targeted on the nation's most critical highway infrastructure*. Washington, DC: United States Government Accountability Office.

Gardoni, P., & Murphy, C. (2014). A scale of risk. *Risk Analysis, 34*(7), 1208–1227.

Goklany, I. M. (2008, February 5). *What to do about climate change.* Policy Analysis, No. 609. Washington, DC: Cato Institute.

Grant, M., & Stewart, M. G. (2012). A systems model for probabilistic risk assessment of improvised explosive device attack. *International Journal of Intelligent Defence Support Systems, 5*(1), 75–93.

Grant, M., & Stewart, M. G. (2015). Probabilistic risk assessment for improvised explosive device attacks causing significant building damage. *Journal of Performance of Constructed Facilities, 29*(5), B4014009.

Grynbaum, M. M. (2014, September 23). At U.N., de Blasio Warns of 'existential threat' from climate change. *New York Times*.

Hall, J. W., Brown, S., Nicholls, R. J., Pidgeon, N. F., & Watson, R. T. (2012). Proportionate adaptation. *Nature Climate Change, 2*, 833–834.

Hardaker, J. B., Fleming, E., & Lien, G. (2009). How should governments make risky policy decisions? *Australian Journal of Public Administration, 68*(3), 256–271.

Hinkel, J., Nicholls, R. J., Vafeidis, A. T., Tol, R. S. J., & Avagianou, T. (2010). Assessing risk of and adaptation to sea-level rise in the European Union: An application of DIVA. *Mitigation and Adaptation Strategies for Global Change, 15*(7), 703–719.

Holden, R., Val, D. V., Burkhard, R., & Nodwell, S. (2013). A network flow model for interdependent infrastructures at the local scale. *Safety Science, 53*(3), 51–60.

IPCC. (2007). Contribution of working groups I, II and III to the fourth assessment report on intergovernmental panel on climate change. In R. K. Pachauari & A. Reisinger (Eds.) (Core writing team), *Climate change 2007: Synthesis report*. Geneva, Switzerland: IPCC.

IPCC. (2012). A special report of working groups I and II of the intergovernmental panel on climate change. In C. B. Field et al. (Eds.), *Managing the risks of extreme events and disasters to advance climate change adaptation.* Cambridge: Cambridge University Press.

Kundzewicz, Z. W., Lugeri, N., Dankers, R., Hirabayashi Doll, P., Pinskwar, I., Dysarz, T., et al. (2013). Assessing river flood risk and adaptation in Europe—Review of projections for the future. *Mitigation and Adaptation Strategies for Global Change, 15*(7), 641–656.

Melchers, R. E., & Jeffrey, R. (2013). Accelerated low water corrosion of steel pilling in harbours. *Corrosion Engineering Science and Technology, 48*, 496–505.

Mueller, J., & Stewart, M. G. (2011a). *Terror, security, and money: Balancing the risks, benefits, and costs of homeland security*. Oxford: Oxford University Press.

Mueller, J., & Stewart, M. G. (2011b). The price is not right: The U.S. spends too much money to fight terrorism. *Playboy, 58*(10), 149–150.

Mueller, J., & Stewart, M. G. (2014). Evaluating counterterrorism spending. *Journal of Economic Perspectives, 28*(3), 237–248.

Mueller, J., & Stewart, M. G. (2016). *Chasing ghosts: The policing of terrorism*. Oxford: Oxford University Press.

Murphy, C., & Gardoni, P. (2008). The acceptability and the tolerability of societal risks: A capabilities-based approach. *Science and Engineering Ethics, 14*(1), 77–92.

Nishijima, K., Maruyama, T., & Graf, M. (2012). A preliminary impact assessment of typhoon wind risk of residential buildings in Japan under future climate change. *Hydrological Research Letters, 6*(1), 23–28.

Norville, H. S., Harvill, N., Conrath, E. J., Shariat, S., & Mallonee, S. (1999). Glass-related injuries in Oklahoma city bombing. *Journal of Performance of Constructed Facilities, 13*(2), 50–56.

NTSB. (2008, November 14). Highway accident report: Collapse of I-35W Highway Bridge, Minneapolis, Minnesota, August 1, 2007. Accident Report NTSB/HAR-08/03. Washington, DC: National Transportation Safety Board.

OMB. (1992). *Guidelines and discount rates for benefit-cost analysis of federal programs (revised)*. Circular No. A-94, October 29, 1992. Washington, DC: Office of Management and Budget.

Paté-Cornell, E. (2002). Risk and uncertainty analysis in government safety decisions. *Risk Analysis, 22*(3), 633–646.

Peng, L., & Stewart, M. G. (2014). Spatial time-dependent reliability analysis of corrosion damage to concrete structures under a changing climate. *Magazine of Concrete Research, 66*(22), 1154–1169.

Risky Business. (2014, June). Risky business: The economic risks of climate change in the United States. RiskyBussiness.org.

Robinson, L. A., Hammitt, J. K., Aldy, J. E., Krupnick, A., & Baxter, J. (2010). Valuing the risk of death from terrorist attacks. *Journal of Homeland Security and Emergency Management, 7*(1).

Stewart, M. G. (2014). Risk and economic viability of housing climate adaptation strategies for wind hazards in southeast Australia. *Mitigation and Adaptation Strategies for Global Change, 20*(4), 601–622.

Stewart, M. G., & Deng, X. (2015). Climate impact risks and climate adaptation engineering for built infrastructure. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering, 1*(1), 04014001.

Stewart, M. G., Ellingwood, B. R., & Mueller, J. (2011). Homeland security: A case study in risk aversion for public decision-making. *International Journal of Risk Assessment and Management, 15*(5/6), 367–386.

Stewart, M. G., & Melchers, R. E. (1997). *Probabilistic risk assessment of engineering systems*. London: Chapman & Hall.

Stewart, M. G., & Mueller, J. (2013). Terrorism risks and cost-benefit analysis of aviation security. *Risk Analysis, 33*(5), 893–908.

Stewart, M. G., & Mueller, J. (2014a). Cost-benefit analysis of airport security: Are airports too safe? *Journal of Air Transport Management, 35*(March), 19–28.

Stewart, M. G., & Mueller, J. (2014b). Risk and cost-benefit analysis of police counter-terrorism operations at Australian airports. *Journal of Policing, Intelligence and Counter Terrorism, 9*(2), 98–116.

Stewart, M. G., & Mueller, J. (2014c). Terrorism risks for bridges in a multi-hazard environment. *International Journal of Protective Structures, 5*(3), 275–289.

Stewart, M. G., & Peng, J. (2010). Life cycle cost assessment of climate change adaptation measures to minimise carbonation-induced corrosion risks. *International Journal of Engineering under Uncertainty: Hazards, Assessment and Mitigation, 2*(1–2), 35–46.

Stewart, M. G., Val, D., Bastidas-Arteaga, E., O'Connor, A., & Wang, X. (2014). Climate adaptation engineering and risk-based design and management of infrastructure. In D. M. Frangopol & Y. Tsompanakis (Eds.), *Maintenance and safety of aging infrastructure* (pp. 641–684). Leiden: CRC Press.

Stewart, M. G., Wang, X., & Willgoose, G. R. (2014). Direct and indirect cost and benefit assessment of climate adaptation strategies for housing for extreme wind events in Queensland. *Natural Hazards Review, 15*(4), 04014008(12).

Stewart, M. G., & Mueller, J. (2011). Cost-benefit analysis of advanced imaging technology full body scanners for airline passenger security screening. *Journal of Homeland Security and Emergency Management, 8*(1), Article 30.

Sunstein, C. R. (2003). Terrorism and probability neglect. *Journal of Risk and Uncertainty, 26*(2–3), 121–136.

Susskind, L. (2010). Responding to the risks posed by climate change: Cities have no choice but to adapt. *Town Planning Review, 81*(10), 217–235.

Sydney Ports. (2008, March). *Port botany container terminal expansion overview*.

Val, D. V., Holden, R., & Nodwell, S. (2013). Probabilistic assessment of failures of interdependent infrastructures due to weather related hazards. In G. Deodatis, B. R. Ellingwood, & D. M. Frangopol (Eds.), *Safety, reliability, risk and life-cycle performance of structures and infrastructure* (pp. 1551–1557). London: Taylor & Francis Group.