Life-Cycle of Structures and Infrastructure Systems – Biondini & Frangopol (Eds)

Risk and decision-making for extreme events: What terrorism and climate change have in common

M.G. Stewart
University of Technology, Sydney, Australia

ABSTRACT: Terrorism and climate change debates are often characterized by worst-case thinking, cost neglect, probability neglect, and avoidance of the notion of acceptable risk. This is not unexpected when dealing with extreme events. However, it can result in a frightened public, costly policy outcomes, and wasteful expenditures. The paper will describe how risk-based and cost-benefit approaches are well suited to infrastructure decision-making in these uncertain environments.

1 INTRODUCTION

Cyclones, earthquakes, tsunami 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'. There is much hyperbole in the media and other sources that terrorism and more recently climate change are (or can be) reaching dangerous levels, are apocalyptic, or even existential. This characterisation of extreme events can result in a frightened public, costly policy outcomes, and wasteful expenditures. Hence, extreme events illicit extreme reactions – risk aversion, probability neglect, cost neglect, worst-case thinking – that may distort the decision-making process in an effort by policy makers to be seen to be 'doing something' irrespective of the actual risks involved.

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 dwell on lists of vulnerabilities and consequences. There is seldom mention of probabilities, or 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.

Civil Engineering infrastructure such as houses, buildings, bridges, roads, pipelines, dams, etc. are vulnerable to terrorism and climate change. Over the past century building standards have been developed and continually improved – with the prevention of building collapse and catastrophic loss (ultimate limit state) the main driver for change. And while uncertainties and knowledge gaps still exist, disaster risks in the developed world are, in general, at an acceptable level. Hence, new infrastructure is, in general, built to modern codes of practice and so are less vulnerable to these extreme events. However, risks are generally higher for ageing or deteriorating infrastructure.

Risk-based approaches are well suited to optimising decisions related to extreme events (e.g., Stewart and Rosowsky 2022), in this case, climate adaptation strategies and counterterrorism measures. Stochastic methods may be used to model threat likelihood, vulnerability, resilience, effectiveness of protective strategies, exposure, and costs. Probabilistic terrorism risk assessment methods have been developed to assess the risks of terrorism, and effectiveness of risk reducing

DOI: 10.1201/9781003323020-10

measures (Mueller and Stewart 2011, 2015). Risk-based assessments of climate adaptation measures have also been developed (e.g., Bastidas-Arteaga and Stewart 2019). While the jargon may differ, the decision support approaches to counterterrorism and climate adaptation measures have much in common, as are the challenges. This paper aims to draw out these issues in more detail, with a particular focus on the pitfalls often encountered when assessing the threats, hazards, vulnerabilities and consequences of counter-terrorism measures, and climate change mitigation and adaptation.

2 CLIMATE ADAPTATION ENGINEERING

In recent years climate change seems to have displaced terrorism as the extreme event of most concern to public and governments. There is increasing research that takes into account the changing climate risks and life-cycle costs in engineering to reduce carbon emissions and/or reduce the vulnerability or increase the resiliency of infrastructure – this may be referred to as '*climate adaptation engineering*'. Climate adaptation engineering is defined as measures taken to:

(i) reduce CO_2 emissions during the life cycle of design, construction, operation and end-of-life of infrastructure that may include decarbonisation measures such as more sustainable (low carbon) materials, enhanced operation efficiency (e.g., more thermally efficient buildings), and changes to inspection and maintenance regimes, and/or
(ii) reduce the vulnerability or increase the resiliency of built infrastructure to storms, floods, fire, heat and other climate hazards, this may include, for example, enhancement of design standards (higher design loads or flood levels), retrofitting or strengthening of existing structures, or use of hazard resistant materials such as fire-resistant cladding.

Figure 1 shows a schematic to help illustrate the concept of climate adaptation engineering.

The political imperative to "act" on climate change is to reduce CO_2 emissions with a recent push for renewable energy, electric vehicles and other sustainability measures. However, while these measures are needed, their impact on the near to mid-term climate-related losses is miniscule. Whereas measures to reduce vulnerability and enhance resiliency of infrastructure provides a more immediate reduction in climate-related losses.

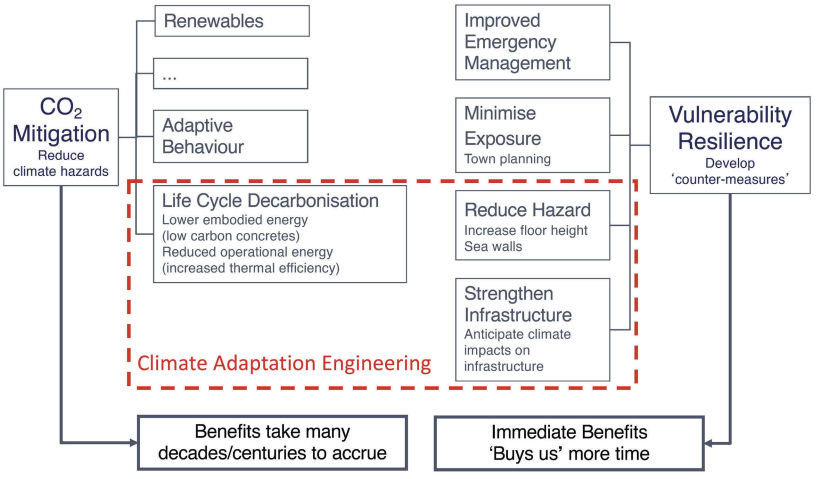

Figure 1. Illustration of climate adaptation engineering.

3 DECISION CHALLENGES: TERRORISM AND CLIMATE CHANGE

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

3.1 *Worst-case thinking*

The media are replete with stories and articles that the world has never been more dangerous, and this is exacerbated by worst-case thinking and hyperbole expressed by 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. In 2021 U.S. President Joe Biden said that climate change poses a "global existential crisis". These are not isolated examples, as similar remarks have been made by Boris Johnson, the United Nations General Secretary, and other world leaders and senior government officials. However, with the exception of all-out nuclear war or an asteroid impacting earth, other threats existential to humanity are 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. It can lead to wasteful expenditures for a threat or hazard that is possible, not probable. Sunstein (2007) notes that "For public officials no less than the rest of us, the probability of harm matters a great deal, and it is foolish to attend exclusively to the worst-case scenario". A more rational approach is to focus on estimating the likelihood of costs and benefits when assessing the need for protective measures. This of course, is the essence of risk assessment.

Worst-case thinking can also lead to excessive spending on programs with little benefit, and ignoring other programs with large benefits. The current U.S. budget for domestic homeland security is approximately $120 billion per year (Stewart and Mueller 2018). Mueller and Stewart (2011) estimated that U.S. counter-terrorism costs are 5-75 times higher than any benefits – i.e., one dollar buys less than 20 cents in benefits. A panel of more than 40 international experts assembled by Bjorn Lomborg found that a $2 billion investment could save more than 1.5 million lives by expanded immunisation coverage and community-based nutrition programs (Lomborg 2009). Hence, if a miserly $2 billion were redirected from the homeland security budget to these more effective risk reducing measures, the likelihood and consequences of terror attacks would hardly change, but 300 to 60,000 more lives would be saved.

3.2 *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.

For example, it is not unusual for books on counter-terrorism to provide exhaustive lists of vulnerabilities and the need for enhanced security measures such as explosive detection systems, surveillance cameras, armed guards, etc. – yet often there is no entry for cost in the index (for examples see Mueller and Stewart 2011).

3.3 *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 U.S. 2014 climate risk assessment report predicts trillions in dollars of damage due to climate change for the business as usual scenario – i.e., the U.S. continues in its current path assuming a RCP8.5 (known more recently as SSP8.5) emission scenario (Risky Business 2014). This IPCC emissions scenario assumes that emissions will continue unabated for the next 85 years including 6.5 more coal being used in 2100 as it is today[1]. This is very much a worse-case scenario, and might be better characterised as unrealistic and implausible as it ignores that CO_2 mitigation measures will be implemented, that adaptation measures are implemented, or the impact of improved or game-changing technologies.

1. A more realistic scenario is RCP 2.6 – this corresponds to the Paris Agreement which aims to hold the increase in the global average temperature to below 2 degrees Celsius above pre-industrial levels.

Sunstein (2003) terms this as 'probability neglect' and 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."

3.4 *Opportunity costs*

Policy-makers 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 U.S. 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 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.

A CO_2 mitigation strategy that reduces economic growth, particularly in developing countries, may reduce their ability to adapt and other indirect impacts. In the 50 years since 1970, the natural hazard fatality rates have reduced by over 90% for low income countries (Ritchie et al. 2022a). This shows that economic development is a key driver in reducing the impact of natural hazards, and climate change mitigation or adaptation measure that reduce economic growth may have a significant opportunity cost.

Further, according to the charity ActionAid, the increased use of industrial biofuels (fuels made on an industrial scale from agricultural crops) have been a major cause of the food and hunger crisis in the developing world – filling an SUV with one tank of biofuel requires over 450 pounds of corn, which contains enough calories for a person for a year (ActionAid 2010). Rising energy costs also mostly affects the poor.

3.5 *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 is 1 in a million (e.g. Stewart and Melchers 1997). The probability that an American will be killed by a hurricane stands at about one in 7 million per year, and one in 2.8 million per year for a heat-related death. The probability that an American will be killed by a terrorist in the United States, with the events of 2001 included in the count, stands at about one in 4 million per year (Mueller and Stewart 2015), and is one in 39 million since 9/11. In Western Europe the odds are higher at one in 9 million, but still considerable lower than one in a million. The annual likelihood worldwide that a person will be killed in an airliner by a terrorist is approximately 1 in 320 million for the period since 9/11. To put some of these data in context, a person would need to fly once per day for 30,000 years before being involved in a terrorist attack (Stewart and Mueller 2018). By comparison, an American's chance of being killed in an automobile crash is about one in 9,500 a year, the chance of being a victim of homicide is about one in 20,000, and the chance of being killed by lightning is one in 10 million (Stewart and Mueller 2018). How much should we be willing to reduce a risk, and is the risk reduction worth the cost?

In the past decade, the chance of being killed in a natural disaster in the United States is one in a million per year, in Western Europe is one in 500,000. However, for the world the odds are significantly higher at one in 150,000 per year (Ritchie et al. 2022b). In the 50 years since 1970, the natural hazard fatality rates have reduced globally by 75%, and by over 90% for low income countries (Ritchie et al. 2022a).

The above data shows that the world is not becoming any more dangerous or vulnerable. There is evidence to suggest that the opposite holds true – it can be argued that the world has never been healthier, wealthier and more educated leading to more resilient societies that can better cope with natural and manmade disasters (for a full discussion see Stewart 2022). While vulnerabilities remain, people and infrastructure are showing increased resilience. Though staggering losses may still occur, they can be ameliorated with targeted strategies to reduce vulnerability, increase resilience or reduce exposure of infrastructure and people to extreme events.

4 LIFE CYCLE ANALYSIS

The decision challenges discussed in the previous section are also mostly relevant for life-cycle analysis for civil engineering infrastructure. These include:

4.1 *Opportunity costs*

Direct costs to an asset owner or manager are, in general, relatively straightforward to estimate for design, construction maintenance, repair, etc. However, opportunity costs are normally harder to quantify and require awareness of unintended impacts to a community. For example, opportunity costs may be considerable if a road or bridge is closed for maintenance and repair, such as delayed response by ambulances reducing the odds of timely life-safety interventions, or occurrence of an extreme hazard (earthquake, bushfire) will hinder emergency vehicle access and safe evacuation routes for residents.

4.2 *Probability neglect*

The world is not deterministic. The timing and severity of natural hazards, loads, deterioration, maintenance, repair, etc. associated with the life-cycle of infrastructure are highly variable and uncertain. Added to this is the uncertainty and incomplete knowledge of how infrastructure is vulnerable and damaged by these hazards, and the ability for economic or societal infrastructure to be resilient and for communities to recover. Infrastructure comprises of interlinked sectors and networks which adds uncertainty about how the performance of each component affects overall system behaviour.

Uncertainty and incomplete knowledge may be modelled by probabilistic (stochastic) methods. It provides a normative measure of uncertainty that may be quantified from field, laboratory or historical data and/or advanced computer simulation models. While the former can help ascertain past or current vulnerabilities and resiliency, it has very little predictive capability if the network or system changes over time to suit increases in demand and shifting community demographics, or if the infrastructure degrades over time, or if the likelihood or severity of natural hazards increases due to climate change. These stochastic methods allow risk to be quantified, such as the likelihood and extent of infrastructure damage and recovery for future scenarios of hazard, vulnerability or resiliency.

An area of particular difficulty for decision-making is where the potential consequences are extremely large or severe yet the probability of these consequences actually occurring is estimated to be extremely low. These are termed “low probability – high consequence” events or hazards, or more recently, as “extreme events”. As discussed above, a probabilistic risk analysis based on sound system and probabilistic modeling is well suited to predicting life saving and damage risks for extreme events. This probabilistic framework provides practical guidance; for example, developing disaster risk reduction measures, safety and load rating assessment of bridges, asset management of pipelines, tunnel safety from vehicle fires, safety cases for offshore platforms and chemical process plants, reliability of electricity infrastructure, and it underpins the development of safety factors and design loads for civil engineering design codes and standards. The next section will describe how risk-based decision support may be applied to life-cycle assessment of infrastructure.

The outcomes of probabilistic risk analysis include: (i) likelihood and extent of infrastructure damage and losses to the owner, users, community and other stakeholders, (ii) influence that infrastructure resiliency has on the time to renewal and follow-on consequences and losses, (iii) effect of risk mitigating measures on predicted damage and losses, and (iv) cost-benefit or similar decision analysis used to assess the probability that a decision option (risk mitigating measure) will yield a benefit to one or more stakeholders. The robustness of decisions can be explored through scenario and sensitivity analyses. Since the outcomes of a probabilistic risk assessment can affect significantly the safety and operations of infrastructure, it is important that an independent and critical review be conducted by recognised experts, and the findings discussed at workshops involving all stakeholders.

Not surprisingly, learned academies such as the Royal Academy of Engineering (RAE) and the Australian Academy of Technological Sciences and Engineering (ATSE) understands the importance of probabilistic thinking: "Regulations and design standards are evidently in need of revision to reflect the uncertain climatic conditions that will be experienced in coming decades, setting probabilistic standards rather than absolute requirements for performance" (RAE 2011) and "The Academy considers evidence-based tools, such as probabilistic risk assessments... to be fundamental for building resilience into Australia's future planning processes" (ATSE 2022). However, they note an understandable concern: "The lack of understanding of probabilistic scenarios by politicians and the media could be particularly problematic" (RAE 2011). This is an ongoing challenge to the engineering profession, where engineers need to explain probabilistic concepts to the government, media and the public in a way that allows for more informed and rational decision-making.

5 RISK-BASED DECISION SUPPORT

Decision criteria for extreme events are typically based on (i) annual fatality risk, and (ii) cost-effectiveness of protective measures. Risk for a system exposed to a threat is

$$E(L)=\sum \Pr(T)\Pr(H|T)\Pr(D|H)\Pr(L|D)L \quad (1)$$

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 effect 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 Equation (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 annual fatality risk (AFR).

If we modify Equation (1) where ΔR is the reduction in risk caused by protective measures (e.g., climate adaptation or counterterrorism measures) then expected loss after protection is

$$E_{protect}(L)=\sum (1-\Delta R)E(L)-\Delta B \quad (2)$$

where ΔR is the reduction in risk caused by the protective measure, E(L) is the 'business as usual' expected loss (risk) given by Equation (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 and/or 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 several 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)

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 net present value (NPV) is equal to benefit minus the cost. The decision problem is to maximise the net present value

$$\mathrm{NPV} = \sum \mathrm{E(L)}\Delta\mathrm{R} + \Delta\mathrm{B} - \mathrm{C_{protect}} \tag{3}$$

where $C_{protect}$ is the protection cost including opportunity costs that reduces risk by ΔR. Figure 2 shows how protective costs increase with risk reduction, while benefits increase. The optimal protection occurs when 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 above discussion is related to the concept of life-cycle cost analysis for infrastructure where design, construction, operation, failure, and end of use costs are summed and the optimal configuration selected based on minimal life-cycle cost or other decision criteria.

Governments and their regulatory agencies normally exhibit risk-neutral attitudes in their decision-making as described by the above equations. Utility theory can be used if the decision maker wishes to explicitly factor risk attitudes such as risk aversion or proneness into the decision process (e.g. Stewart et al. 2011, Qin and Stewart 2021).

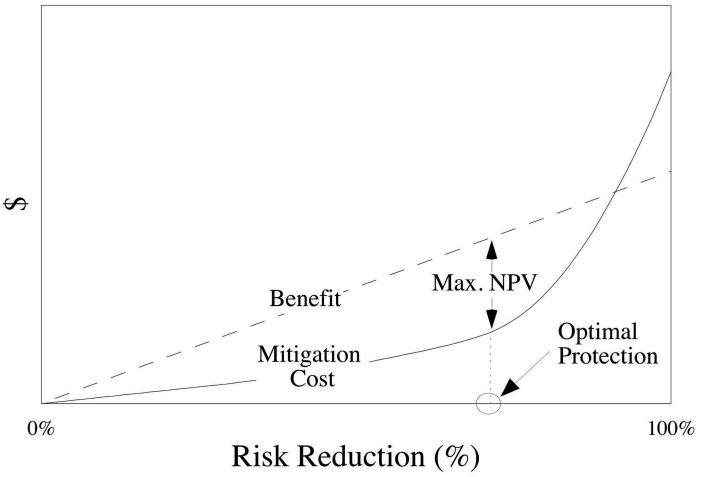

Figure 2. Schematic of net present value (NPV) showing optimal protection.

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) is also variable. This allows confidence bounds of NPV to be calculated, as well as the probability that an adaptation measure is cost-effective denoted herein as Pr(NPV>0). If NPV>0 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 NPV.

If the probability that a specific threat will occur Pr(T) is too unreliable, then a decision analysis based on scenario analysis where threat probability is decoupled from Equation (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 'break-even' 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. mean(NPV)=0. For example, if the actual cost of protection exceeds the predicted break-even value, then protection is not cost-effective. Decision-makers can then judge whether a protective strategy meets these break-even values.

Ultimately however, the outcomes of risk-informed decision analysis will be to inform decision makers as not all decisions can be made on technical merits alone. It also helps to inform government, infrastructure asset and network owners and operators, community and individuals of the trade-offs between risk, benefits and cost when making decisions on how best to protect communities.

6 CONCLUSIONS

Terrorism and climate change are extreme events that engender fear and anxiety in the community. Policy makers 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.

REFERENCES

ActionAid (2010), *Meals per Gallon: The impact of industrial biofuels on people and global hunger*, ActionAid UK, London, United Kingdom.

ATSE (2022), *Building a Resilient Australia*, Position Statement, Australian Academy of Technological Sciences and Engineering. Melbourne, Australia. October.

Bastidas-Arteaga, E. and Stewart, M.G. (2019), *Climate Adaptation Engineering: Risks and Economics for Infrastructure Decision-Making*, Elsevier, Oxford, U.K.

Blalock, G., Kadiyali, V. and Simon, D.H. (2007) The Impact of Post- 9/11 Airport Security Measures on the Demand for Air Travel. *Journal of Law and Economics* 50(4) November: 731–755.

Lomborg, B. (2009). *Global Crises, Global Solutions*, Cambridge University Press, UK.

Mueller, J. and Stewart, M.G. (2011) *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security*. Oxford University Press, Oxford and New York.

Mueller, J. and Stewart, M.G. (2015) *Chasing Ghosts: The Policing of Terrorism*. Oxford University Press, Oxford and New York.

Qin, H. and Stewart, M.G. (2021), Risk perceptions and economic incentives for mitigating windstorm damage to housing, *Civil and Environmental Engineering Systems*, 38(1),1–19.

RAE (2011), *Engineering the Future: Infrastructure, Engineering and Climate Change Adaptation – ensuring services in an uncertain future*, The Royal Academy of Engineering, London.

Ritchie, H., Rosado, P. and Roser, M. (2022a), Natural Hazards, Published online at OurWorldinData.org. https://ourworldindata.org/grapher/decadal-average-death-rates-from-natural-disasters?country=~Low-income+countries (accessed 8 January 2023).

Ritchie, H., Rosado, P. and Roser, M. (2022b), Natural Hazards, Published online at OurWorldinData.org. https://ourworldindata.org/grapher/decadal-average-death-rates-from-natural-disasters?country=~OWID_WRL (accessed 8 January 2023).

Risky Business (2014), Risky Business: The Economic Risks of Climate Change in the United States. RiskyBussiness.org, June 2014.

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

Stewart, M.G. and Melchers, R.E. (1997) *Probabilistic Risk Assessment of Engineering Systems*. London. Chapman & Hall.

Stewart, M.G., Ellingwood, B.R. and Mueller, J. (2011) Homeland Security: A Case Study in Risk Aversion for Public Decision-Making. *Int. Journal of Risk Assessment and Management* 15(5/6):367–386.

Stewart, M.G. and J. Mueller. 2018. *Are We Safe Enough? Measuring and Assessing Aviation Security*, Elsevier, New York.

Stewart, M.G. and Rosowsky, D.V. (2022), *Engineering for Extremes: Decision-making in an Uncertain World*, Springer, Cham, Switzerland.

Stewart, M.G. (2022), Systems Thinking Averts Apocalypses Now and in the Future: Why we should always look on the bright side of life, *Civil Engineering and Environmental Systems*, 39(3): 188–204.

Sunstein, C.R. (2003), Terrorism and Probability Neglect. *J. of Risk and Uncertainty*. 26(2–3):121–136.

Sunstein, C.R. (2007), *Worst-Case Scenarios*. Harvard University Press, Cambridge, MA.