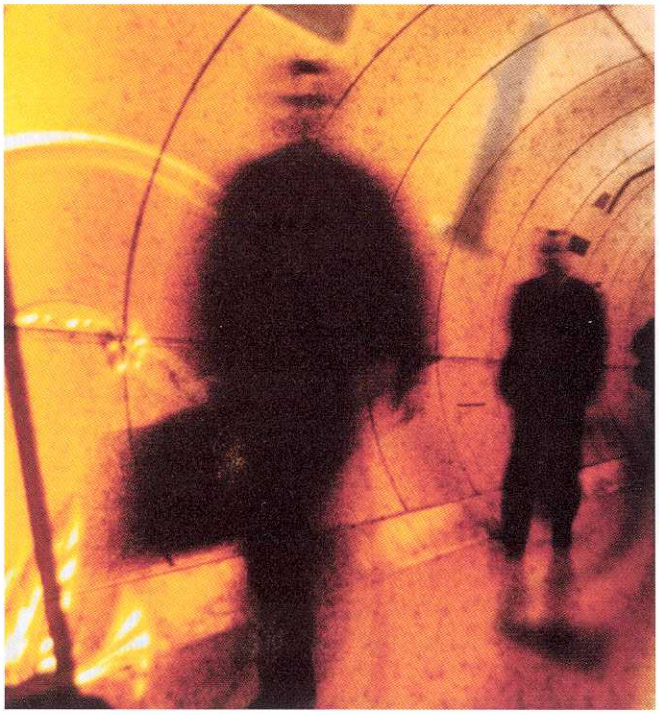
Can Terrorism Risk be Quantitatively Modelled?

With much interest from insurers in coming to terms with the potential of terrorism risk, it is useful to consider what parallels, if any, there might be between estimating the impacts of terrorism threats and conventional methods of assessing catastrophe risk due to natural hazards such as tropical cyclone, flood or earthquake.

By Dr Bruce Harper



Can terrorism be modelled? Some aspects: definitely *yes,* but with considerable uncertainty. Other aspects: probably *no,* at least not in a framework that could benefit traditional insurance planning.

This article sets out some of the reasons for this belief, beginning with a review of the traditional catastrophe risk assessment process applied to natural hazards and contrasting that against the terrorism threat. Some potential alternative methodologies are then also discussed.

Traditional natural hazard catastrophe risk assessment

For the purposes of illustration, the traditional catastrophe risk assessment process can be reduced to a simple four step process:

Step 1: Define the hazard

This involves accumulating knowledge about the nature of the hazard, its space and time scales and potential range of intensity. In the context of tropical cyclones, this means gaining an understanding of their complex dynamic behaviour, spatial structure and how these can interact to produce extreme wind speeds and devastating coastal storm surges.

Step 2: Determine the vulnerability

In this step, the property at risk is identified and classified according to both its location and its likely resistance to the applied catastrophic impacts. In the case of earthquake risk this would involve sub-soil conditions, proximity to fault lines and the structural response to ground acceleration. In respect of cyclonic winds, the height of the property, its exposure and resistance to strong winds needs to be assessed.

Step 3: Assess the likelihood

This next step traditionally requires knowledge about the *climatology* of the risk, i.e. how the risk might vary both in space and time relative to where the property is located. This is typically done by sampling from an historical record of the incidence of, e.g. tropical cyclone tracks, seismic records and the like. Importantly, it is normally implicit that the sampled time series is statistically *stationary,* meaning that the underlying cause of the phenomenon remains static and that the observed record is therefore a random sample from a fixed range of possible outcomes[1].

Step 4: Estimate the impact

All elements can then come together to provide a *quantitative* estimate of the catastrophe risk. The characteristics of the hazard are combined with the vulnerability of the property to predict a range of *deterministic* outcomes, which are then transferred into a statistical or *probabilistic* framework, typically involving stochastic modelling. The accuracy of the outcome is dependent on the individual component accuracies of the deterministic and probabilistic components. The results can then be aggregated and collated to provide information to insurers that will assist in both the design of reinsurance layering as well as longer term portfolio risk mitigation.

Terrorism risk assessment

Following the traditional approach for natural hazard risk assessment:

Step 1: Define the hazard

According to the US State department, the term *terrorism* means 'premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience'. The keywords here from a risk assessment perspective are: *premeditated, non-combatant* and *audience* – all of which significantly differentiate terrorism risks from natural hazards. Ironically, individual terror hazards are clearly difficult to identify due to the very broad range of possibilities. The manifestation of the threat could range across, for example, assassination, siege, hostage-taking, hijacking, sabotage, explosion, contamination etc. The spatial extent of the threat can also cover a wide scale, conceivably from the individual (property or person) through to the metropolis and possibly beyond, depending on the means and the intent. The nature of such risks has been chronicled, not in the scientific journals like natural hazards, but in the newspapers and political history of our societies. It began as a recognisable modern anthropogenic phenomenon, by one assessment[2], around the time of the Jewish terrorist offensive against British rule in Palestine in 1945.

Step	Task	Natural Hazards	Terrorist Hazards
1	Define hazards	Easily identifiable	Difficult to specifically identify
2	Determine vulnerability	Generally classifiable	Wide potential exposure but very specific impacts
3	Assess likelihood	Stationary statistical time series analyses	Non-stationary, externally driven and deliberate
4	Estimate impact	Simulate and aggregate	Simulate and aggregate

TABLE 1. Contrasting the catastrophe risk assessment process.

Step 2: Determine the vulnerability

There is a near-limitless range of potential terrorist targets in a free society. It seems axiomatic that our very freedoms provide the ready access and opportunity needed to commit such acts. In many ways terrorism, akin to crime, is a threat of opportunity, albeit requiring considerable planning but, depending on the intent, often only modest resources. A society's only reactive defence is apparently intelligence and vigilance. The US State Department's definition does, however, provide some guidance in narrowing down the more likely targets, namely the *non-combatant* and *audience* ingredients. This immediately points to preferably iconic civilian targets having a high visibility, and also a high potential impact. Regrettably, the desired impact in this context is *terror*, best manifested by large-scale innocent loss of life, preferably live on television. The next best outcomes from a terrorist perspective are then likely *fear* of loss of life and/or large scale social and/or economic disruption that directly or indirectly follows.

Step 3: Assess the likelihood

This is where the *climatology* of the risk needs to be specified. Unfortunately there is no direct analogy here with natural hazards – terrorism is clearly *non-stationary*, externally driven and *deliberate*. The terrorist threat cannot be readily represented in a manner akin to a natural hazard. Notwithstanding this, some analysis techniques can be brought to bear in relative contexts, as explored later.

Step 4: Estimate the impact

In contrast, this step is potentially relatively straightforward and largely analogous to the natural hazard assessment. In summary, as per Table 1, terrorist risk assessment needs deviate most significantly from those for natural hazard risks in Steps 1 and 3. Step 2, while broad, is capable of more rational assessment.

Determining the vulnerability

We can readily examine the many aspects of our societal vulnerability and the attractiveness of potential targets to terrorists:

Damage to community and society icons

This includes public institutions, monuments, religious sites and buildings. These are highly visible targets but will generally yield low loss of life and have mostly symbolic impact overall.

Large city office buildings

These are highly visible and offer the dual attractiveness of high human density and easy accessibility. There is also the possibility of high levels of collateral damage through fire, collapse etc. The September 11 attack at the World Trade Center clearly represents the ultimate execution of such a threat.

Stadiums/conference venues/entertainment

These are the oft-called *soft* targets, where a large concentration of people could lead to the highest likelihood of deaths. There is the added attraction of high visibility through television coverage. In the extreme, such attacks are also likely to be highly socially destabilising, leading to many citizens boycotting public places.

Transportation systems

One of the greatest personal fears remains the possibility of in-flight hijacking or explosion, although much greater potential loss of life could likely be caused on the ground at airports. The highest potential mortality in the transport sector would be underground railways. Their combination of large passenger numbers, high service frequency and restricted evacuation options yields a high risk index. In terms of long-term serious disruption leading to economic losses, the greatest

vulnerabilities in the transport sector would be large bridges, tunnels (e.g. the English Chunnel) and shipping canals, such as the Suez and Panama. The means needed to affect some of these large-scale facilities would be considerable, but possible.

Dams

Large dams are highly visible and the public has a natural fear of dam break. In practice, however, probably few dams worldwide threaten large populations and dam-break flood waves are not as spectacular as Hollywood portrays, except in very close proximity to the breach. Even the famous *Dam Busters* had limited impact on the German war effort in 1943 and few economies rely on hydropower to any significant extent. Also, most dams are massive and highly stable, being built to withstand large natural forces such as earthquakes. The effort required to breach such facilities would probably not justify the outcomes, even if successful.

Power generation and distribution systems

These are highly vulnerable to specific attack from conventional explosive devices and if well planned and executed could lead to massive failures of individual installations. Loss of electric power for any period more than a few days has a very significant economic impact, e.g. Auckland in 1998. With the added danger of radiation release, nuclear power stations probably offer the greater terrorist attraction.

Water supply

Water supply authorities around the world have probably stepped up their security over recent years but this sector remains one of the most highly vulnerable to some form of attack. Firstly, water supply systems were never designed for high levels of security, representing an age of innocence where the greatest threat was conceived as ingress of vermin or catchment pollution. Wire fences and padlocks are all that protect the vast majority of water supply networks, which offer a multitude of points of attack. Without back-flow preventers, any domestic tap represents a possible point of entry into the water supply system. The extent to which large scale attacks could practically be executed however remains a moot point. The dilution issue is rarely publicly debated but a well-sighted entry point could probably affect an office building or a portion of a neighbourhood. However, fear is again is likely to be the main outcome: Sydney's supposed brush with *Cryptosporidium* and *Giardia* contamination in 1998 showed the very high level of disruption that can occur.

Atmospheric substance release

Leaving aside the possibility of a nuclear bomb, this is the oft-reported *doomsday* scenario, whereby either nuclear (dirty bomb), chemical or biological agents might be dispersed over a metropolis or larger sized areas, potentially affecting many tens or hundreds of thousands of people. By way of illustration, even though the current SARS virus outbreak is a natural mutation, it highlights the extreme vulnerability of a society accustomed to a high level of international travel.

Foodstuff contamination

Perhaps somewhat lower on the radar but still possible, would be concerted attempts to contaminate bulk foods such as grain, livestock or manufactured goods. The 'Panadol' and 'Arnott's' extortion cases alone caused considerable social concern and economic losses, while the current Pan Pharmaceuticals product recall potentially highlights how easy it could be, in similar circumstances, for a malevolent person to contaminate products and have them widely distributed.

Fossil fuel supplies

This remains a highly vulnerable sector due to the typically remote environments and the volatility of the product. There is the added terrorist advantage of such attacks being highly visible and to likely have international impact, at least on the money markets. There is also the potential for long-term disruption that could initiate further crises or adverse environmental effects, e.g. the Iraq/Kuwait disaster in 1991.

Assessing the likelihood

Notwithstanding the difficulty of the overall problem of quantifying the risk of terrorism, there are many tools and techniques available to partially address sub-components of risk that could be of benefit to the insurance sector. These might include: system stability analyses to assess overall facility or institutional resilience, facility fault or event tree analyses, safety indexing methods, scenario and simulation techniques, risk based design to minimise losses, mathematical games theory, human and organisational analysis to assess threat profiles and reactions.

Mostly, such techniques need to step back from the concept of a holistic threat and concentrate instead on the premise that *if a terrorist attack has occurred*, what is the probability that the impact on such-and-such a system will be within certain limits? This provides a significant simplification of the problem that can lead to the development of relative quantitative risks being estimated. However, it leaves aside the vexed issue of the absolute risk, which is always likely to be problematic and subject to almost daily revision by security agencies. Regardless of which of these techniques might be able to be used, all implicitly rely on ***data*** – a concept shared with the natural hazards problem. Some of these techniques and their data needs are briefly discussed below.

System stability analyses

We can think conceptually of any entity as a *system* in a black-box sense, reacting to external stimuli, in this case a terrorist attack. The concepts of unconditionally stable and unconditionally unstable systems (refer Figure 1) lead to two extremes of behaviour; the former much more desirable than the latter. In practice, natural *systems*, whether structural, mechanical, political, economic, organisational etc., are a combination of these features and can be deemed *meta-stable*, meaning stable under certain conditions. System stability analysis seeks to determine the behaviour of the overall system in terms of combinations of these constructs and looks for *detection* and *response* feedbacks that monitor the overall system stability. This is an abstract concept, but one that can be used to begin to understand the otherwise seemingly impossible complexity of some situations and how a terrorist stimuli might be handled and mitigated against.

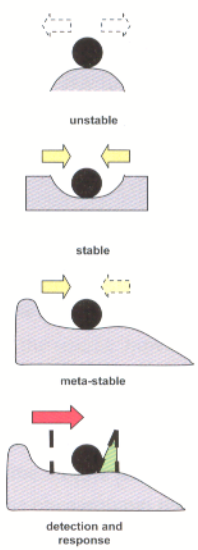


FIGURE 1. System Stability Concepts.

Facility fault or event tree analysis

This is an analytical approach that can directly address the detailed impacts of *what if* sequences of events. For example, Figure 2 illustrates how a threat to a power station might be assessed as a sequence of failure events, each with an estimated probability and cost, linked to a possible mode of attack. The total probability of a given level of loss could be dependent on the vulnerability of the fuel source used (e.g. hydro, coal, fuel oil or gas) and the particular physical layout of a particular plant. The time to repair could depend on factors such as the process complexity, fuel stocks or availability of parts. Such techniques are routinely used in the petrochemical industry for assessing process risks. By including terrorism risk, it could be possible for a facility owner to demonstrate to an insurer how it has planned to minimise its losses in such an event or what steps it plans to mitigate possible losses through redesign, augmentation or increased security of facilities.

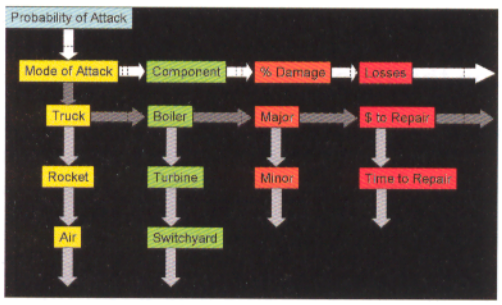


FIGURE 2. Example fault tree event analysis for a terrorist attack on a power station.

Scenario analysis

This technique is typically applied where there is considerable uncertainty about the possible range of risk and is akin to the traditional 'design storm' concept. It remains the only technique currently considered by the *International Panel on Climate Change*, when considering possible worldwide impacts of the so-called Enhanced Greenhouse effect. In the terrorism context, specific major attacks would be devised and their effects modelled mathematically. For example, complex numerical atmospheric models can be used to predict the path and dilution of aerial contaminants under a range of pre-considered conditions.

Risk based design

This approach is most commonly associated with the US space program (NASA) but has been in use in many industries over the past decades. It is a quantitative method that, in the terrorism context, can be used to develop a model of a security system and balance the threats against a range of mitigation proposals. For example, it could be used to estimate the cost (in $, disruption, loss of freedom etc.) involved in lowering the potential number of fatalities from a nuclear bomb detonation in a major seaport. The cost of the increased scanning, quarantine, random searches and trans-shipment time can then be compared with the reduction in estimated fatalities.

Game theory

Recently popularised in the movie *A Beautiful Mind*, where the life of Nobel prize-winner John Nash was portrayed, game theory is a highly complex mathematical construct that seeks to establish an optimal strategy for a player, given a set of resource constraints and an opponent with likewise intent. While Nash considered economic theory, technically it can be applied to terrorism and, if successful, might lead to the best chance of providing a quantitative threat index, say, for a nation at a particular instance in time. In simple terms, game theory would consider the range of potential targets, their attractiveness to terrorists and the state's ability to detect or optimally defend against attack. It is likely that governments are already using such analyses, although the advantage for insurers is uncertain as one needs to be a player in the game to influence it. It might, however, be a potential technique for the internal minimisation of losses across a portfolio that has terrorist exposure.

Human and organisational factors

Knowledge of terrorist group behaviour is clearly of interest to national security organisations. However, similar knowledge of the human behaviour of individual state and city administrations, specific companies, employers and employees is also crucial in estimating the possible outcomes of a terrorist attack. Such factors as the extent to which decision-making is delegated and access to resources may assist insurers in assessing the style of attacks that might affect a facility and the relative likelihood of effective defence.

Conclusion

Can terrorism risks be quantitatively modelled? Yes, with time, data and expertise, insurers can expect to have access to detailed deterministic analyses on the one hand, simple aggregations of risks, or relative quantitative risks on an industry or regional basis. Scenario-driven probabilistic outcomes are also a possibility that could sway underwriting decision-making and enable products for market.

It is unlikely that probabilistic assessments of terrorist risks will ever be on par with natural hazards assessments. The industry should also expect that detailed analyses for major classes of risk (involving time and expertise) would be relatively expensive, at least in the first instance. Fairly broad estimates from spatial averaging models will probably emerge over time but it is likely there will be a slow development of plausible probabilistic models. In the longer term, if terrorism persists, the most relevant insurance rating analogy might simply be burglary and theft, unfortunately based on claims experience! ■

Dr Bruce Harper is a specialist civil engineer in the field of natural hazards risk analysis and is Managing Director of Systems Engineering Australia Pty Ltd (SEA) based in Brisbane.

The author wishes to acknowledge assistance from colleagues at Risk Engineering Inc (Boulder, Colorado) and SAIC (McLean, Virginia) in the preparation of the original RDG Seminar, upon which this paper is based.

[1] It is worthwhile noting that, in the context of possible anthropogenic climate change, the stationarity principle is already under some threat in respect of natural hazards.

[2] Centre for Defence & International Security Studies, Department of Politics and International Relations, Lancaster University UK, http://www.cdiss.org