

## **BENEFIT-COST ANALYSES FOR MALEVOLENT HUMAN ACTIONS**

Note prepared for the Columbia/Penn Roundtable  
Palisades, New York, April 12-13, 2002

*By Dr. Gordon Woo*

*Risk Management Solutions  
Gordon.Woo@rms.com*

Human nature being what it is, there is a wide range of malevolent ways in which individuals or groups of people can cause damage, injuries or fatalities. These criminal actions include burglary, robbery, vandalism, sabotage, arson and terrorism. Accepting that criminal action is not easy to express in a quantitative language, if it is a salient factor, it should be incorporated into benefit-cost analyses. In mid-February 2002, a newly built refugee detention center in England was badly damaged by arson. The rebuilding cost of more than \$50 million may be set against the comparatively modest expense of a fire sprinkler system which was not installed on financial grounds, even though recommended by the local Fire Department. Defenders of this financial decision might argue that the probability of an arson attack was unknowable. However, the occupants of the detention center were all earmarked for deportation, having had their application for asylum rejected. An elicitation of expert judgement as to the likelihood of an arson attack would have been helpful before turning down the sprinkler system.

In this example, only the public sector was involved. But, in general, the societal cost of protection against criminal action is shared between the public and private sectors. The relative balance of risk is a quandary which couples together diverse security interests: heightened anti-terrorism policing after September 11 has diverted police resources to such an extent as to lead to a large increase in street crime in London. This note outlines some benefit-cost issues embedded in the public-private security partnership.

Given the level of policing provided by the state, deciding on extra security involves weighing up the residual risk. If there is a constant police patrol outside a property, there may be no need for a burglar alarm. However, if this patrol is withdrawn, then installation of a burglar alarm, or even hiring a local security officer, may be a wise course of action. This may be the simplest paradigm for the impact of malevolent human actions, yet even in this example there are some intriguing decision strategy issues. In their analysis of interdependent security, Kunreuther and Heal have considered the implications of installing a burglar alarm, when some other neighborhood properties are unprotected. The chance of your property being robbed is reduced, but the chance of your neighbor being robbed may be increased. Quantitative analysis of this case study requires use of some concepts of game theory.

Another form of petty crime is vandalism, much of which is committed by juveniles. This becomes serious when human life is threatened. A disturbing example is the action of children in dropping concrete blocks from UK railway bridges onto roads below. The cost to the railway company of raising parapets to protect the bridges would be enormous; the benefit would be the saving of several lives per year. A benefit-cost argument, invoking a notional monetary value of a human life, has been successfully employed to argue with the UK safety regulator against the need for such anti-vandalism expenditure.

Sabotage by disgruntled employees is a special concern for manufacturing industry. Where statutory risk limits are imposed on a hazardous plant, the impact of an internal act of sabotage might well be to violate these limits. This violation might satisfy the saboteur's objective of embarrassing if not distressing plant management. Measures are taken by management to make operations as sabotage-proof as possible, but increasing levels of security incur an ever increasing cost. Risk assessments at some UK nuclear installations are made to maximize the benefit of anti-sabotage expenditure.

In UK, anti-terrorism expenditure has been substantial over the past few decades in meeting the IRA threat to potential military, government, and civilian targets. The cost of terrorist action on the mainland, and the burden of providing protection, has been borne by both the public and private sector. In their terror campaign, the IRA have aimed strikes at many different types of British target: from the Prime Minister's residence to the Palace of Westminster, to bridges, highways, subway stations, commercial offices, department stores, hotels and pubs. Extra security for government buildings, (such as an entrance gate into Downing Street), and additional police guards, have served to mitigate the risk to this class of target. However, transport infrastructure is notoriously hard to protect, and bomb scares alone caused weekly disruption of the London subway system.

Given the priority of providing security for government property, it is inevitable that police and military resources should be concentrated around this task. This leaves most industrial, commercial and residential property exposed to some residual terrorism risk that can be partially mitigated through adopting, and paying for, additional security measures. But as the burglar alarm paradigm demonstrates, risk mitigation strategies may involve game-theoretic insights in even the most basic adversarial situations.

What are the implications of alternative strategies for security enhancement? Consider one particular class of target, known to be attracting the al-Qaeda network: US nuclear power plants. These plants are of different ages, sizes and types of construction, and have different degrees of vulnerability to terrorist attack. Underground plants would be inherently safer from both accidental and malicious sources of hazard, but such designs are still on the drawing board. What is the optimal defensive strategy, recognizing that the terrorist adversary has his own adaptive attack strategy?

The most glaring vulnerability of nuclear plants is to impact from large aircraft. In nuclear safety cases, this scenario is usually ruled out on the grounds of improbability as an accident: aircraft crashes are rare, and pilots are expected to make every effort to

avoid hitting built-up areas. The most serious near-miss arose when the ill-fated Pan-Am jet disintegrated over Lockerbie, under the force of a terrorist bomb, only a few kilometers from the Chapelcross nuclear plant near the England-Scotland border. With the future prospect of kamikaze attacks on nuclear plants, the best defence is a shield of fighter jets, or anti-aircraft missile launchers, prepared to shoot down planes straying too close to a nuclear plant. These military assets could be collectively deployed in such a way as to prevent any one plant from being significantly more vulnerable to kamikaze attack than another.

Where civil decisions are made to prevent commercial jets from being hijacked or stolen, there will be vulnerability differences between airlines and airports. The installation of bullet-proof cockpit doors is a safety precaution which some airlines have invested in so as to win back the confidence of anxious passengers as well as deter would-be hijackers. Those airlines which are slow to introduce improved security measures may become more likely targets. As with airlines after September 11, commercial airports are under economic pressure to save expenditure where possible. Recently, Manchester airport in northwest England announced that it was cutting the jobs of a number of security staff in response to the downturn in air travel. Enticed by this publicity, a journalist succeeded in smuggling weapons passed security barriers at this airport.

The meticulous planning of the attacks of September 11 recognized the geographical and temporal variation in airport security. To the extent that a security lapse at one airport may compromise the future of many airports, and that no security system can be terrorist-proof, the benefit-cost issue of collective security is important. Minimum standards may be set by regulators, but weaknesses in security at certain specific airports are unlikely to be missed by terrorists. Ranking of airports according to security standards would give an indication of relative terrorist hazard. This would be similar to the existing ranking of international airports according to landing difficulty and accident risk.

As with airports, so also with sea ports, there are varying standards of security protection against acts of piracy and the use of large vessels as destructive impact weapons. Increasingly, quantitative risk assessments are undertaken for commercial ports, and these assessments should allow for malevolent as well as accidental damaging human actions. Again, the ranking of major ports according to standards of security should provide insight into the relative likelihood of some high-profile ports being targeted rather than others.

For any class of infrastructure or type of property, differences in security between potential targets may be exploited by vigilant terrorists. The global nature of the al-Qaeda threat makes for interdependent international security. If all but a few major members of a class undergo a significant security upgrade, those which are more vulnerable may become exposed to higher hazard. A simple illustration would be famous international landmark structures. In London, one of the most popular tourist attractions is the London Eye ferris-wheel, which was built to celebrate the new millennium. Through illegal sit-ins, this attraction has already become a focal point of direct political action. Given the perceived threat of a massive IRA bomb, the

foundations of the London Eye were especially designed at the outset to be bomb-proof. There are much easier landmark targets for terrorists than this.

How much is it worth spending to make another international landmark less vulnerable? From a purely economic benefit-cost standpoint, this is an intriguing, if hypothetical, question. Leaving terrorism insurance out of the equation, the expense of reconstruction and business interruption after an attack may be estimated by engineers and accountants. But to quantify the benefit requires some attempt at gauging the likelihood of a terrorist attack. This may be split into the frequency of attacks on major landmarks, and the conditional probability that one specific landmark is designated for a given attack. The overall frequency may be elicited from experts, knowledgeable about the relative proportions of terrorist attacks on different classes of targets (e.g. 15% diplomatic; 50% commercial; etc..).

The conditional probability that one specific landmark is attacked will depend partly on its relative vulnerability, and partly on its intrinsic attractiveness as a political totem. The former may be established from information on construction, maintenance and security; the latter may be elicited from experts on international terrorism. Whether managers have to decide on strengthening a structure; or increasing security to reduce the chance of a successful attack; or purchasing terrorism insurance cover, some idea of event likelihood is needed for intelligent benefit-cost analysis.