Terrorism Risks for Bridges in a Multi-Hazard Environment.

by

Mark G. Stewart, John Mueller

Reprinted from

International Journal of

Protective Structures

Volume 5 · Number 3 · September 2014

Multi-Science Publishing

ISSN 2041-4196

Terrorism Risks for Bridges in a Multi-Hazard Environment

Mark G. Stewart[1*] and John Mueller[2*]
[1]Professor and Director, Centre for Infrastructure Performance and Reliability The University of Newcastle New South Wales, 2308, Australia
[2]Senior Research Scientist, Mershon Center for International Security Studies Ohio State University
Senior Fellow, Cato Institute, Washington, D.C.

Received on 23 Oct 2013, Accepted on 27 Apr 2014

ABSTRACT
The paper will assess terrorist threats to new and existing bridges and the cost-effectiveness of protective counter-terrorism measures. This analysis will consider threat likelihood, cost of security measures, risk reduction and expected losses to compare the costs and benefits of protective measures to bridges to decide which protective measures are cost-effective. In this paper, a break-even cost-benefit analysis determines the minimum probability of an attack, absent the protective measures, that is required for the benefit of the protective measures to equal their cost for new and existing bridges. It was found that unless terrorist threat probabilities are high, then typical protective measures are not cost-effective. Bridges and other critical infrastructure are subject to a range of natural and man-made hazards, and terrorism is most likely not as important a threat as natural hazards. It was found that economic risks to bridges from floods, earthquakes, and ship impact are higher than threats from terrorism.

Keywords: terrorism, risk, bridges, cost-benefit analysis, safety

1. INTRODUCTION

Many reports and studies have highlighted the vulnerability of critical infrastructure to terrorism, and over the past 20 years terrorists have targeted buildings, bridges, pipelines, and aviation infrastructure. The preferred method of attack is Improvised Explosive Devices (IEDs), and there is much research and interest into assessing the vulnerability and strengthening of bridges subject to IEDs (e.g., [1–4]). Most recently, this has resulted in publication of the 2011 AASHTO Bridge Security Guidelines [5].

There are 600,000 highway bridges in the United States, a vital part of a transportation system that supports 86% of all personal travel and 80% of the nation's freight. Moreover, bridges are - or seem to be - especially vulnerable. As Chairman Bennie Thompson of the

*Corresponding author. *Email address*: mark.stewart@newcastle.edu.au, bbbb@osu.edu

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." [6]. However, a bridge is very difficult to damage severely because its concrete and steel construction makes it something of a hardened structure from the outset. Building facades (glass, masonry, cladding) are far more vulnerable [7]. There seems to be little evidence terrorists have any particular desire to blow up a bridge, due in part, perhaps, to the facts that it is an exceedingly difficult task under the best of circumstances and that the number of casualties is likely to be much lower than for many other targets. The issue, then, is to evaluate how, and to what degree, society has been benefited by the protection of bridges.[1]

The cumulative increase in expenditures on U.S. domestic homeland security over the decade since 9/11 exceeds one trillion dollars, see Mueller and Stewart [8, 9]. Up to 45% of this expenditure is devoted to protecting critical infrastructure and key resources. Yet there is little evidence that such expenditures have been efficient. A significant challenge is balancing the costs and benefits of counter-terrorism measures when the threat scenarios are highly transient and there is considerable risk averseness by decision-makers [10]. To compare costs and benefits requires the quantification of threat probability, risk reduction, losses, and security costs (e.g. [11–27]). Much of this work can be categorised as 'probabilistic terrorism risk assessment'.

It was understandable, in the years immediately following the terrorist attacks of September 11, 2001 that there was a tendency to spend in haste on homeland security. Yet, in the intervening 13 years, little scientific rigour has been applied to assess the effectiveness of this expenditure. There is a need to examine homeland security expenditures in a careful and systematic way, applying the kind of system and reliability modelling approaches that are routinely applied to other hazards. This type of rigour, where security and public policy decisions are assessed on technical, social and economic considerations of risk acceptability, is needed to ensure that public funds are expended on measures that maximise public safety. Terrorism may be viewed as a 'new hazard', that although different in nature from other hazards, requires systems and reliability approaches similar to those adopted to other hazards to assess risk and safety [11, 27].

NHCRP [4], Williamson and Winget [1], and others all recommend that counter-terrorism (CT) protective measures only be implemented if they are cost-effective. However, little guidance is provided on how to achieve this goal. The U.S. Government Accountability Office and Congress have repeatedly urged the U.S. Department of Homeland Security (DHS) to undertake risk and cost-benefit assessments of major programmes [28, 29]. A review by RAND [30] revealed a number of key deficiencies in DHS risk management. Among them it: "does not attempt to describe the absolute risks to the system, rather just the relative risks, or changes in magnitude of risk". A key component of assessing absolute risk is including the probability of an attack in the calculations, whereas a relative risk assessment is often conducted conditional on an attack occurring and then ranking risks based on the relative likelihood of threats. Hence, the paper will assess terrorist threats to bridge infrastructure and the cost-effectiveness of CT protective measures. The analysis will consider threat likelihood, cost of security measures, risk reduction and expected losses to

[1]There may be co-benefits to bridge protection, such as reassuring the travelling public or reducing the risks from seismic, flood, vehicle impact, or other hazards. Co-benefit is considered in Eqn. (2).

compare the costs and benefits of protective measures to bridges to decide which protective measures are cost-effective. A break-even cost-benefit analysis determines the minimum probability of an attack, absent the protective measures, that is required for the benefit of the protective measures to equal their cost. Where possible, we use actual or representative threat, consequence and cost data, and will assess the cost-effectiveness of protective measures for (i) new bridges, and (ii) retrofitting existing bridges. The intention of the examples is to show the methodology of risk acceptance criteria and not to make any definitive conclusions. This paper uses single point estimates of threat likelihood, risk reduction, and losses because there is little probabilistic information available for these parameters for bridge protection. They are also sufficient to illustrate the decision framework, and to provide an initial first-pass or risk screening of the cost-effectiveness of bridge CT protective measures. For details on the probabilistic characterisation of threat, risk reduction, and losses for buildings and aviation infrastructure see Stewart [24, 25] and Stewart and Mueller [19–21].

Bridges and other critical infrastructure are subject to a range of natural and man-made hazards, and terrorism is most likely not nearly as important a threat to them as are natural hazards. Economic risks due to terrorism are then compared with risks from flood, seismic, and shipping impact hazards.

2. RISK-BASED DECISION SUPPORT

The definition of risk adopted by the DHS and risk analyses for many applications is [31–33]:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequences} \tag{1}$$

An appropriate decision analysis compares the marginal costs of CT protective measures with the marginal benefits in terms of fatalities and damages averted. In other words, the benefit is the reduction in risk. The decision problem is to maximise the net present value (equal to benefits - cost) or net benefit:

$$\text{NPV} = E(C_B) + \sum \Pr(T)\Pr(H|T)\Pr(L|H)L\Delta R - C_{\text{security}} \tag{2}$$

where

- $E(C_B)$ is the expected co-benefit from the security measure not directly related to mitigating terrorist threats (e.g. reduced vulnerability to earthquakes, reduction in vandalism).
- Threat:
  - Pr(T) is the annual probability of an attack per item of infrastructure - ie. the likelihood a terrorist attack will take place if the security measure were not in place.
- Vulnerability:
  - Pr(H|T) is the conditional probability of a hazard (successful initiation/detonation of an IED, or other initiating event leading to damage and loss of life) given occurrence of the threat, Pr(L|H) is the conditional probability of a loss given occurrence of the hazard.
- Consequences L is the loss or consequence.
- Reduction in risk (ΔR) is the degree to which the security measure foils, deters, disrupts, or protects against a terrorist attack.
- C_{security} is the extra cost of CT protective measures including opportunity costs.

The summation sign in Eqn. (2) refers to the number of possible threat scenarios, hazard levels and losses. A protective measure is viewed as cost-effective or efficient if the net benefit exceeds zero. Equation (2) can be generalised for any time period, discounting of future costs and more detailed time-dependent cost and damage consequences.

Although we understand that people are often risk averse when considering issues like terrorism, we follow current U.S. Office of Management and Budget and other government requirements that governments expending tax money in a responsible manner need to be neutral when assessing risks, something that entails focusing primarily on mean estimates in risk and cost- benefit calculations, not primarily on worst-case or pessimistic ones [34, 35]. However, Eqn. (2) can be generalised for expected utility incorporating risk aversion (e.g. [36]).

Terrorism is a unique threat because it may arise from an intelligent adversary who will adapt to changing circumstances to maximise likelihood of success. Yet many terrorists are neither intelligent nor particularly adaptive as one might expect. For example, Kenney [37] finds that Islamist militants in Spain and the UK are operationally unsophisticated, short on know-how, prone to make mistakes, poor at planning, and limited in their capacity to learn (see also [38, 39]). Other studies document the difficulties of network coordination that continually threaten operational unity, trust, cohesion, and the ability to act collectively (e.g. [40]). It is true, of course, that some terrorist attacks are carefully planned. However, for many terrorist target selection effectively becomes something like a random process [8]. In most cases, target selection may not have been random in their minds but would essentially be so in the minds of people trying to anticipate their next move.

Equation (2) can be simplified by assuming that vulnerability is $\Pr(H|T) = \Pr(L|H) = 100\%$ and co-benefit $E(C_B) = 0$. Hence, a break-even analysis to calculate how many attacks would have to take place to justify the expenditure gives

$$p_{\text{attack-min}} = \frac{C_{\text{security}}}{L\Delta R} \tag{3}$$

In this approach the threat probability is the output of the cost-benefit analysis and it is the prerogative of the decision-maker, based on expert advice about the anticipated threat probability, to decide whether or not a security measure is cost-effective.[2]

The quantification of vulnerabilities and risk reduction is not straightforward, but 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 is recommended if appropriate data are available. Sensitivity analyses are essential to test the robustness of the decision to uncertainties in input parameters. We recognise that Eqn. (2) is a simplification, however, it is a useful starting point for further discussion and perhaps for more detailed and complex analysis of how to manage the often conflicting societal preferences associated with assessments of risk, cost, and benefits (for a full discussion see Mueller and Stewart [8]). To be sure, Eqns. (2) and (3) can be expanded to consider multiple threats, losses, and risk reductions, and to characterise these variables stochastically (e.g., [24, 25]). However, these often have little influence on the final decision, and for bridges, the main threat of interest is a large IED as evidenced by the large number of reports that discuss this particular threat.

[2]For example, if the break-even attack probability $p_{\text{attack-min}}$ is calculated to be 50% per bridge per year, and if the actual threat is estimated to be 0.01 – 5% per bridge year, then even though the anticipated threat probability is very uncertain, it clearly falls below the 50% threshold by an order of magnitude. In this case, protection is not cost-effective.

Clearly, risk and cost-benefit considerations should not be the sole criterion for public decision making. Nonetheless, they provide important insights into how security measures may (or may not) perform, their effect on risk reduction, and their cost-effectiveness. They can reveal wasteful expenditures and allow limited funds to be directed to where the most benefit can be attained. More important, if risk and cost-benefit advice is to be ignored, the onus is on public officials to explain why this is so, and the trade-offs and cuts to other programs that will inevitably ensue [27].

3. HIGHWAY BRIDGES

While there are numerous instances throughout the world in which buildings have been attacked by terrorists, there are very few reported attacks on bridges, suggesting that any supposed threat to highway bridges may well be overblown even though bridges (like a near-infinite number of other targets) may be vulnerable to attack in some sense. An analysis of terrorism incidents compiled by the Global Terrorism Database (GTD) shows that in the ten year period 1998 to 2007 there were only two 'successful' attacks on bridges in the UK - all IRA sponsored, generating only minor damage and no fatalities. Over the same period of time there were none at all in continental Europe or North America [41]. Moreover, worldwide only 5% of guerrilla and terrorist attacks on public surface transportation systems in the 80-year period from 1920 to 2000 were directed at bridges and tunnels, and only 1% were so attacked during the last three and half years of that period [42]. Bridges have been the target of some terrorist activity in Iraq and Afghanistan, but these are war zone situations where bridges may have an attractive tactical value for insurgents.

In principle, an IED is relatively simple to design and manufacture if done by well trained personnel, resulting in reliabilities in excess of 90% [43]. However, the probability of an IED creating a damaging effect (casualties) reduces to 19% for terrorists in Western countries where there is less opportunity for IED operational skills to be acquired [43]. This was clearly evident from the second attack on the London Underground on 21 July 2005 where four IEDs failed to initiate, and on Glasgow international airport in 2007 and Times Square in 2010 where Vehicle Borne Improvised Explosive Devices (VBIEDs) failed to detonate. The probability of successful attacks using IEDs increases to 65% for terrorists or insurgents in the Middle East [43]. Our assumption of $Pr(H|T) = 100\%$ is very generous indeed.

Most highway bridges are two to four lanes wide with spans of 30 to 50 m crossing rivers, roads, and railway lines. An American Society of Civil Engineers (ASCE) Task Committee considers an upper bound practical threat from a single-rear-axle delivery vehicle to be a 2,000 kg TNT VBIED [44]. Others suggest that smaller explosives, on the order of 250 kg, could cause "catastrophic damage" to a typical U.S. highway bridge [45, 46]. There is no doubt that VBIEDs (or accidental blast loads) can cause bridge collapse, as evidenced by the 2013 collapse of an 80 m expressway bridge in China caused by the accidental explosion of a truck carrying fireworks that also killed 14 people. Yet even a massive VBIED may fail to totally collapse a bridge, or even cause too much disruption. Photos of damage caused by a huge VBIED, reputedly up to 5 tonnes, detonated on a highway bridge near Ramadi, Iraq, on October 17, 2009, show collapse of only one lane of one span (see Figure 1), and the bridge seems to have been quickly reopened [47]. In addition, there were no casualties. Similarly, an attack on a 10 m bridge in the Khyber Pass was repaired and reopened within 72 hours (Figure 2). 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 perished in any single attack [41].

Figure 1. Vehicle Borne Improvised Explosive Device Damage to Bridge in Iraq (47).

An explosive blast will not always 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 recently completed 10-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 [48]. 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 [49]. 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.

Because highway bridges have a large variety of spans, widths, geometry, etc., it is difficult to generalize about damage costs. However, several case studies of recent U.S. bridge collapses may be instructive. The replacement and demolition costs for two damaged U.S. interstate highway bridges were $4 million and $11.75 million, for bridges in Los

Figure 2. Damage to Bridge in Khyber Pass (66)

Angeles from $6.2 million to more than $60 million, and for the I35W bridge in Minneapolis $234 million [50]. We set replacement costs for a typical interstate highway bridge at $20 million [51]. Traffic diversion and associated user delay costs for a bridge under construction can total $430,000 per day, which, even in the case of a rapid bridge replacement in Oklahoma of only 46 days, amounted to nearly $20 million [52].

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. We will assume this causes a loss of $100 million, and we assume that the expected number of fatalities is twenty, at a cost of $130 million based on value of statistical life of $6.5 million [53]. 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 and existing bridges typically focus on strengthening columns and girders by fibre reinforced polymers (FRPs), additional steel reinforcement, minimum dimensions, adding lateral bracing, and increasing stand-off by bollards, security fences, and vehicle barriers (e.g., [2, 4]). Although there is much information available about design and retrofitting bridges to mitigate the effects of blast damage [1, 3, 54] there is little information about their cost. However, buildings and bridges are similar structural systems in terms of vulnerability, and so require similar protective measures. The National Academy of Sciences reports that for newly constructed commercial office buildings in the United States, "reasonable blast resistance can be accomplished for about a 5% premium in construction cost" [54], and another study concludes that "substantial protection may be afforded by an increase in overall costs of the order of 5% to 10%." [55]. This includes only the costs of reducing a building's vulnerability to damage by structurally hardening it. Perimeter security fences 300 m long cost $120,000, a single bollard up to $26,000, and vehicle crash barriers $70,000 [56]. Expenses mount further with the addition of security guards, closed-circuit televisions, and alarm and communication systems.

3.1 DESIGN OF NEW BRIDGES

We will assume 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. Annualized over a design life of 75 years at a 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 $C_{security}$=$50,000 per year.

As for the reduction in risk element in Eqns. (2) and (3), we will generously assume that protective measures reduce the risk by a substantial $\Delta R = 95\%$. We also assume 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 (Section 3 shows that Pr(H|T) is more likely to be 19%), and that the blast will then cause bridge collapse and maximum consequences (L). In other words, we assume that every attack will achieve 100% success. These assumptions are substantially biased in favour of showing that security measures are cost-effective.

As suggested earlier, the likelihood of a terrorist attack on a highway or railway bridge in western nations is remote. Engineering and design issues suggest that bridges should not be an attractive target for terrorists, and incident data suggest they are not. Table 1 shows the annual

attack probabilities ($p_{attack\text{-}min}$) required at a minimum for security expenditures on protecting a bridge to be cost-effective. This break-even 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 0.02% or one in 5,000 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 0.04% per bridge. If the average cost of construction is halved to only $10 million per bridge, then $C_{security}$ is halved to $25,000, but if losses remain at $250 million then Table 1 shows that the annual attack probability needs to exceed 0.01% per bridge per year for CT protective measures to be cost-effective.

If the likelihood of a VBIED detonation is taken as Pr(H|T) = 19% as obtained from the GTD [43], then break-even attack probabilities shown in Table 1 will increase more than five-fold. And if bridge vulnerability is reduced to a more realistic Pr(L|H) = 50% then break-even attack probabilities shown in Table 1 will increase ten-fold. These more realistic assumptions reduces the cost-effectiveness of bridge protection considerably. On the other hand, the co-benefit of CT protective measures may be considerable if strengthening a bridge to be more blast-resistant has the co-benefit of reducing the risks from seismic, flood or other hazards. In this case, break-even attack probabilities would reduce.

If there were one attack on a highway bridge every year in the United States, the attack probability would be only 1 in 600,000 per bridge per year (0.0002%) because there are 600,000 bridges in the country. Ellingwood [57] suggests that the minimum attack probability may be higher at 0.01% for buildings with high density occupancies, key governmental and international institutions, monumental or iconic buildings or other critical facilities with a specific threat. It should be noted that although the probability of a terrorist attack in the U.S. or elsewhere may be high, the probability that any particular item of infrastructure will be attacked is very low. These probabilities are much lower than the 0.02% likelihood of a successful attack required for new bridge protective measures to be cost-effective. If the attack probability is a high 0.01% per bridge per year then the

Table 1. The probability of an otherwise successful terrorist attack, in percentage per year, required for protective security expenditures to be cost-effective ($p_{attack\text{-}min}$), assuming the expenditures reduce the risk of an attack by 95 percent

	Losses from a Successful Terrorist Attack (L)					
Cost of security measures (per year)	**$100 million**	**$250 million**	**$1 billion**	**$2 billion**	**$10 billion**	**$100 billion**
$25,000	0.026	0.01	0.003	0.0013	0.0003	0.00003
$50,000	0.05	0.02	0.005	0.0026	0.0005	0.00005
$100,000	0.1	0.04	0.011	0.005	0.001	0.0001
$250,000	0.3	0.11	0.026	0.013	0.003	0.0003
$500,000	0.6	0.21	0.053	0.026	0.005	0.0005
$1 million	1.1	0.42	0.105	0.053	0.011	0.0011
$5 million	5.3	2.10	0.526	0.26	0.053	0.0053
$10 million	10.5	4.20	1.05	0.53	0.11	0.0110
$100 million	105.3	42.1	10.5	5.26	1.05	0.1060

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

benefit-to-cost ratio is only 0.48 - i.e., $1 of cost buys 48 cents of benefits. In fact, the only threat against a U.S. highway bridge in the U.S. since 9/11 (that we know of) was a terrorist plot (foiled in the planning stages) to target the four lane Brecksville-Northfield High Level Bridge near Cleveland, Ohio in 2012.[3]

If lives saved is the only criterion for risk acceptability, protective measures would save only 0.0019 lives per year when the attack probability is below 0.01% per bridge per year. The cost per life saved (cost of protection divided by lives saved) exceeds $26 million and thus fails a cost- benefit assessment because this is far in excess of the value of statistical life of $6.5 million.

Finally, it may seem prudent to provide CT protective measures for new bridges as the additional cost for a single bridge may seem modest at something like $50,000 per bridge per year, or a 5% increase in construction costs. The ASCE 2013 Infrastructure Report Card recommends that $20.5 billion is needed annually to replace or repair existing bridges in the U.S. [58]. Up to an additional $2 billion per year in funding would then be needed to provide CT 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 - such as flood levee banks, tornado shelters, or other infrastructure to reduce risks from natural hazards (e.g., [8]).

3.2. RETROFITTING EXISTING BRIDGES

Strengthening existing structures is considerably costlier. An upper bound broad estimate may be obtained from examining retrofit costs for bridges damaged by earthquakes because the stresses on the bridge are not dissimilar to those caused by explosions. The retrofit cost for the historic Cesar Chavez highway bridge in Los Angeles was 15% of its replacement value, and a "full-blown" rehabilitation of a U.S. four-span steel girder bridge was 51.5% of its replacement value [46,59,60].

We will conservatively assume that substantial mitigation of blast effects can be achieved at a cost of 10% of a bridge's replacement value - i.e., at a cost less than for seismic retrofitting. If the bridge replacement value is $20 million, the cost of strengthening it is then $2 million. Annualized over a remaining service life of five to 20 years at a 4% discount rate, a middle value for strengthening resulting in a security cost of $C_{security}$ = $250,000 per year. The break-even analysis in Table 1 shows that protective measures would be cost-effective only if the probability of a successful terrorist attack without them exceeds 0.11% or one in 900 per bridge per year. Clearly, retrofitting existing bridges is less cost-effective than designing new bridges to be blast-resistant.

If there is a specific threat such that the likelihood of attack increases, or if a bridge is deemed an iconic structure such that its perceived value is 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, as evidenced by the embryonic plot in 2002 to use blowtorches to sever the cables of the Brooklyn Bridge [39].

---

[3]The 2002 plot to destroy the Brooklyn Bridge was more fanciful than a serious threat. Mueller (2013) summarises the threat as "in 2002, Iman Faris traveled to New York City under orders from Khalid Sheikh Mohammed to survey possible terror targets within the United States. After basic internet research Faris decided on the Brooklyn Bridge as a potential target and believed that 'gas torches' could be used to bring the bridge down. However after conducting physical reconnaissance of the bridge (which consisted of driving over it once), Faris concluded that an attack was unlikely to succeed because of the bridge's structural design and because of the New York Police Department patrols there, and he never sought to acquire the equipment necessary for such an attack." There may be other threats that we are unaware of, but the threat level is likely to be less than one threat per year.

Concerns about this led a blue ribbon panel on bridge and tunnel security to inform the Federal Highway Administration in 2003 that "preliminary studies indicate that there are approximately 1,000 [bridges] where substantial casualties, economic disruption, and other societal ramifications would result from isolated attacks," that the "loss of a critical bridge or tunnel at one of the numerous 'choke points' in the highway system could result in hundreds or thousands of casualties, billions of dollars worth of direct reconstruction costs, and even greater socioeconomic costs," that the "ordinary cost of construction to replace a major long-span bridge or tunnel on a busy interstate highway corridor in the United States may be $1.75 billion," and that, summing reconstruction costs and socioeconomic losses, the "loss of a critical bridge or tunnel could exceed $10 billion." [54]. An accompanying cost analysis of protective measures for four large U.S. bridges concludes that the cost to protect these bridges ranges from $20.6 to $157.4 million. If the average cost of $95.6 million is annualized over a 25-year period, it comes to $5.5 million per year.

We can evaluate the panel's conclusion by referring again to Table 1. Applying the panel's expected losses of $10 billion with protective costs rounded down to $5 million per year, the attack probability would need to exceed 0.05%, or 1 in 2,000, per bridge per year. Taking the panel's estimate of 1,000 critical U.S. bridges, this would mean that terrorists would otherwise be able to successfully conduct a (truly) massive attack on one of these bridges at least once every two years for these protective costs to be cost-effective. The evidence to date suggests that such a high attack probability is not being observed. See Mueller and Stewart [8] for further details.

3.3. DISCUSSION

The results of the cost-benefit assessment suggest that many bridges require no protective measures as they cannot be classified as 'critical' to society. So while 'critical infrastructure protection' is a worthy goal, many individual items of infrastructure are likely to fail to be 'critical' to the nation or the economy. However, there may be some 'key resources' - defined by the U.S. government as 'publicly or privately controlled resources essential to the minimal operations of the economy or government' [61] - that might warrant protective measures. This might include, for example, monuments and iconic structures such as the Golden Gate Bridge, Empire State Building, Brooklyn Bridge, Washington Monument, etc. as well as nuclear power plants, dams and government facilities. The protection of 'key resources' should also be subject to rigorous cost and benefit assessments as many thousands of individual assets would meet the definition of 'key resources' and a need still exists for optimal resource allocation for their protection.

We are applying historical data here of course, and it could be argued that they do not necessarily provide a reliable guide to the future. However, those making that argument need to explain why the capacity of terrorists to commit damage will increase in the future and why terrorists will become more likely to target bridges than they have in the past. To date, there is little evidence that terrorists are becoming any more destructive, particularly in the West, and fears about large, sophisticated attacks have been replaced by ones concerning tiny conspiracies, lone wolves, and one-off attackers [8, 38].

There is an argument that protecting infrastructure maybe prudent and worthwhile because the threat levels may increase, thus increasing the benefit of protective measures over time. This has some merit. However, it assumes that protective measures is the only way to foil terrorism. Yet infrastructure protective measures are only the 'last line of defence'. The FBI and other police and intelligence services (and tip-offs from the public) are responsible for foiling or preventing most terrorist plots [39]. These police and security

services deal with all terrorism threats, almost certainly do reduce the terrorism threat, and can be rapidly deployed or re-deployed as threats emerge or evolve. They are thus likely to be more cost-effective than attempts to protect thousands (if not millions) of potential infrastructure targets.

Finally, we are not arguing that protecting bridges may be wasteful because we believe there will be no more terrorist attacks. Like crime and vandalism, terrorism will always be a feature of life, and a condition of zero vulnerability is impossible to achieve. However, future attacks might not be as devastating as 9/11, as evidenced by the attacks on Western targets in the 12 years since 9/11 that, although tragic, each have claimed victims numbering in the tens to a few hundred. The frequency and severity of terrorist attacks are low, which makes the benefits of enhanced CT infrastructure protection challenging to justify by any rational and accepted standard of cost- benefit analysis.

4. COMPARISON OF TERRORIST RISKS WITH OTHER HAZARDS

If the annual attack probability is 1 in 600,000 per bridge per year, and economic loss is $250 million, the annual expected loss (risk) is only $420 per year for a typical U.S. highway bridge. A ten-fold increase in attack probability leads to an annual expected loss of $4,200 per year. By means of broad comparison, mean economic risks which are also referred to as expected annual losses (EAL), are estimated for three significant hazards to typical bridges in the United States: floods, earthquake, and ship impact.

The economic risk due to bridge scour ranges from $940 (Nebraska) to $23,690 (Massachusetts) per bridge in the U.S. [62]. While Deco and Frangopol [63] estimate expected annual losses of approximately $13,000 per year. These losses include rebuilding costs, vehicle running costs, time loss costs, and cost of lost life.

Annual seismic losses for 45 m steel and concrete bridges range from $3,600 to $25,000 for central and southeastern U.S. locations [64]. The risks may more than double for more active seismic regions of the United States, such as the west coast [64].

Ship impact to an historic inland river bridge in Germany causes a probability of collapse of 0.5% per year [65]. For a bridge valued at $80 million considering replacement value and user delay costs [24], this equates to an annual economic risk of $400,000 per year.

Evidently, for many locations bridge flood, earthquake, and impact risks are higher than the terrorism risks estimated herein. These comparisons of risks between terrorism and natural hazards provide useful insights into hazards that dominate risks to society. In all cases, it would be more rational to direct limited resources to flood, seismic, and ship impact risk mitigation rather than to terrorist protective measures if the threat is nonspecific.

5. CONCLUSIONS

The cost-effectiveness of protective and counter-terrorism measures for bridges considered threat likelihood, cost of security measures, risk reduction and expected losses. A break-even cost- benefit analysis determines the minimum probability of an attack, absent the protective measures, that is required for the benefit of the protective measures to equal their cost. If there are no co- benefits, it was found that unless terrorist threat probabilities are high, then typical protective measures are not cost-effective for new and existing brides. For example, a break-even analysis shows that retrofitting protective measures for an existing bridge that cost $250,000 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 0.1% or one in 1,000 per bridge per year. It was found that economic risks to bridges from floods, earthquakes, and ship impact are higher than

threats from terrorism. The co-benefit of CT protective measures may be considerable if strengthening a bridge to be more blast-resistant has the co-benefit of reducing the risks from seismic, flood, vehicle impact, or other hazards. In this case, there is higher likelihood of CT protective measures being cost-effective.

Finally, this paper provides a starting point for further discussion. The assumptions and quantifications made here can be queried, and alternate data or hypotheses can be tested in a manner which over time will minimize subjectivity and parameter uncertainty inherent in an analysis for which there are little accurate data. This should lead to more widespread understanding and agreement about the relative cost-effectiveness of bridge counter terrorism protective measures.

ACKNOWLEDGEMENTS

The support of the Australian Research Council is gratefully acknowledged. Professor Mueller appreciates the financial support of a Distinguished Scholar Award at Ohio State University.

REFERENCES

[1] Williamson, E.B. and Winget, D. (2005), Risk Management and Design of Critical Bridges for Terrorist Attack, *Journal of Bridge Engineering,* 10(1): 96–106.

[2] Winget, D., Marchand, K., and Williamson, E. (2005). Analysis and Design of Critical Bridges Subjected to Blast Loads. *Journal of Structural Engineering,* 131(8): 1243–1255.

[3] Williamson, E.B. and Marchand, K. (2006), Recommendations for Blast-Resistant Design and Retrofit of Typical Highway Bridges, *Proceedings of the 2006 Structures Congress,* American Society of Civil Engineers, CD-ROM.

[4] NHCRP (2010), *Blast-Resistant Highway Bridges: Design And Detailing Guidelines,* NCHRP Report 645, National Cooperative Highway Research Program, Transportation Research Board, Washington, DC, 2010.

[5] AASHTO (2011) *Bridge Security Guidelines,* American Association of State Highway and Transportation Officials, Washington, DC.

[6] GAO (2009), *Federal Efforts to Strengthen Security Should Be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure,* United States Government Accountability Office, Washington, DC.

[7] Norville, H.S., Harvill, N., Conrath, E.J., Shariat, S. and Mallonee, S. (1999), Glass-Related Injuries in Oklahoma City Bombing, *Journal of Performance of Constructed Facilities* 13(2): 50–56.

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

[9] Mueller, J. and Stewart, M.G. (2011), The Price is Not Right: The U.S. spends too much money to fight terrorism, *Playboy*, 58(10): 149–150.

[10] Mueller, J. (2006), *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them,* Free Press, New York.

[11] Stewart, M.G., Netherton, M.D. and Rosowsky, D.V. (2006), Terrorism Risks and Blast Damage to Built Infrastructure, *Natural Hazards Review,* ASCE, 7(3): 114–122.

[12] Stewart, M.G. and Netherton, M.D. (2008), Security Risks And Probabilistic Risk Assessment of Glazing Subject to Explosive Blast Loading, *Reliability Engineering and System Safety,* 93(4): 627–638.

[13] Netherton, M.D. and Stewart, M.G. (2009), The Effects of Explosive Blast Load Variability on Safety Hazard and Damage Risks for Monolithic Window Glazing, *International Journal of Impact Engineering,* 36(12): 1346–1354.

[14] Netherton, M.D. and Stewart, M.G. (2010), Blast Load Variability and Accuracy of Blast Load Prediction Models, *International Journal of Protective Structures*. 1(4): 543–570.

[15] Dillon, R.L., Liebe, R. and Bestafka, T. (2009), Risk-based Decision Making for Terrorism Applications, *Risk Analysis,* 29(3): 321–335.

[16] Cox, L.A. (2009), Improving Risk-Based Decision-Making for Terrorism Applications, *Risk Analysis*, 29(3): 336–341.

[17] Stewart, M.G. and Mueller, J. (2008), A Risk and Cost-Benefit and Assessment of U.S. Aviation Security Measures, *Journal of Transportation Security,* 1(3): 143–159.

[18] Stewart, M.G. and Mueller, J. (2008), A Cost-Benefit and Risk Assessment of Australian Aviation Security Measures, *Security Challenges,* 4(3): 45–61.

[19] Stewart, M.G. and Mueller, J. (2011), Cost-Benefit Analysis of Advanced Imaging Technology Fully Body Scanners for Airline Passenger Security Screening, *Journal of Homeland Security and Emergency Management,* 8(1): Article 30.

[20] Stewart, M.G. and Mueller, J. (2013), Terrorism Risks and Cost-Benefit Analysis of Aviation Security, *Risk Analysis*, 33(5): 893–908.

[21] Stewart, M.G. and Mueller, J. (2013), Aviation Security, Risk Assessment, and Risk Aversion for Public Decisionmaking, *Journal of Policy Analysis and Management,* 32(3): 615–633.

[22] Willis, H. and LaTourette, T. (2008), Using Probabilistic Terrorism Risk-Modeling for Regulatory Benefit-Cost Analysis: Application to the Western Hemisphere Travel Initiative in the Land Environment, *Risk Analysis,* 28(2): 325–339.

[23] Stewart, M.G. (2008), Cost-Effectiveness of Risk Mitigation Strategies For Protection of Buildings Against Terrorist Attack, *Journal of Performance of Constructed Facilities,* ASCE, 22(2): 115–120.

[24] Stewart, M.G. (2010), Acceptable Risk Criteria for Infrastructure Protection, *International Journal of Protective Structures*, 1(1): 23–39.

[25] Stewart, M.G. (2010), Risk-Informed Decision Support for Assessing the Costs and Benefits of Counter-Terrorism Protective Measures for Infrastructure, *International Journal of Critical Infrastructure Protection,* 3(1): 29–40.

[26] Sewart, M.G. (2011), Life Safety Risks and Optimisation of Protective Measures Against Terrorist Threats to Infrastructure, *Structure and Infrastructure Engg*. 7(6): 431–440.

[27] Mueller, J. and Stewart, M.G. (2014), Terrorism and Counterterrorism in the US: The Question of Responsible Policy- Making, *International Journal of Human Rights,* 18(2): 228–240.

[28] GAO (2011), *Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11,* U.S. Government Accountability Office, Washington, D.C.

[29] Rogers, M. (2012), *Rebuilding TSA into a Smarter, Leaner Organization,* A Majority Staff Report - Subcommittee on Transportation Security Committee on Homeland Security, 112th Congress, September 2012.

[30] Morral, A.R., Price, C.C., Oritz, D.S., Wilson, B., LaTourrette, T., Mobley, B.W., McKay, S., and Willis, H.H. (2012), *Modeling Terrorism Risk to the Air Transportation System,* RAND, Santa Monica, CA.

[31] NRC (2010), *Review of the Department of Homeland Security's approach to risk analysis*. National Research Council of the National Academies, National Academies Press, Washington, DC.

[32] Kaplan, S. and Garrick, B.J. (1981), On the quantitative definition of risk, *Risk Analysis,* 1: 11–27.

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

[34] OMB (1992), *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs (Revised),* Circular No. A-94, October 29, 1992, Office of Management and Budget, Washington, DC.

[35] OBPR (2010), *Best Practice Regulation Handbook,* Office of Best Practice Regulation, Australian Government, Canberra, June 2010.

[36] Stewart, M.G., Ellingwood, B.R. and 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.

[37] Kenney, M. (2010), 'Dumb' yet Deadly: Local Knowledge and Poor Tradecraft among Islamist Militants in Britain and Spain, *Studies in Conflict and Terrorism,* 31:1–22

[38] Mueller, J. and Stewart, M.G. (2012), The Terrorism Delusion: America's Overwrought Response to September 11, *International Security* 37(1): 81–110.

[39] Mueller, J. (2013), *Terrorism Since 9/11: The American Cases*. http://politicalscience.osu.edu/faculty/jmueller/since.html

[40] Brooks, R.A. (2011), Muslim "Homegrown" Terrorism in the United States: How Serious is the Threat? *International Security,* 36(2): 7–47.

[41] GTD (2010), Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism, University of Maryland, United States.

[42] Jenkins, B.M. and Gersten, L.N. (2001), *Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices*, Mineta Transportation Institute, San José State University, MTI Report 01-07, September 2001.

[43] Grant, M. and 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.

[44] Conrath, E.J., Krauthammer, T., Marchand, K. and Mlakar, P. (1999), *Structural Design for Physical Security: State of the Practice,* ASCE, Reston, VA.

[45] Islam, A. K. M. A. and Yazdani, N. (2006), Blast Capacity and Protection of AASHTO Bridge Girders, *Proceedings of the 2006 Structures Congress,* American Society of Civil Engineers, CD-ROM.

[46] Seible, F., Henemier, G., Karbhari, V.M., Wolfson, J., Arnett, K., Conway, R. and Baum, J.D. (2008), Protection of Our Bridge Infrastructure against Man-Made and Natural Hazards. *Structure and Infrastructure Engineering* 4(6): 415–429.

[47] AP (2009), Truck Bomb Destroys Key Bridge in Western Iraq, *Associated Press,* 17 October 2009.

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

[49] Bai, Y., Burkett, W. and Nash, P. (2006), Lessons Learnt from the Emergency Bridge Replacement Project, *Journal of Construction Engineering and Management,* 132(4): 338–344.

[50] Foti, J. (2008), 35W Bridge on Pace to Open in September, *Star Tribune,* May 4, 2008.

[51] Luna, R., Hoffman, D. and Lawrence, W.T. (2008), Estimation of Earthquake Loss due to Bridge Damage in the St. Louis Metropolitan Area. I: Direct Losses, *Natural Hazards Review,* 9(1): 1–11.

[52] Bai, Y. and Burkett, W. (2006), Rapid Bridge Replacement: Processes, Techniques, and Needs for Improvements, *Journal of Construction Engineering and Management,* 132(11): 1139–1147.

[53] 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).

[54] NAS (1995), *Protecting Buildings from Bomb Damage: Transfer of Blast-Effects Mitigation Technologies from Military to Civilian Applications,* National Academy of Sciences, National Academy Press, Washington, DC.

[54] FHWA (2003), Blue Ribbon Panel on Bridge and Tunnel Security, *Recommendations for Bridge and Tunnel Security,* Federal Highway Administration, September 2003.

[55] Smith, P.D. and Hetherington, J.G. (1994), *Blast and Ballistic Loading of Structures,* Butterworth-Heinemann, Oxford.

[56] RSMeans (2003), *Building Security: Strategies and Costs,* Reed Construction Data, 2003.

[57] Ellingwood, B.R. (2006), Mitigating Risk from Abnormal Loads and Progressive Collapse, *Journal of Performance of Constructed Facilities,* 20(4): 315–323.

[58] ASCE (2013), 2013 Infrastructure Report Card, American Society of Civil Engineers, March 2013.

[59] Kuprenas, J.A., Madjidi, F., Vidaurrazaga, A. and Lim, C. (1998), Seismic Retrofit Program for Los Angeles Bridges. *Journal of Infrastructure Systems* 4(4): 185–191.

[60] Wang, E. (2006), Optimizing Bridge Seismic Retrofit Strategy Implementing Bridge Fragility Curves, *Proceedings of the 2006 Structures Congress,* American Society of Civil Engineers, CD-ROM.

[61] DHS (2009), *National Infrastructure Protection Plan,* Department of Homeland Security, Washington, D.C.

[62] Khelifa, A., Garrow, L.A., Higgins. M.J. and Meyer, M.D. (2013), Impacts of Climate Change on Scour-Vulnerable Bridges: Assessment Based on HYRISK, *Journal of Infrastructure Systems,* 19(2): 138–146.

[63] Deco, A, and Frangopol, D.M. (2011), Risk Assessment of Highway Bridges Under Multiple Hazards, *Journal of Risk Research,* 14(9): 1057–1089.

[64] Ghosh, J. and Padgett, J.E. (2011), Probabilistic seismic loss assessment of aging bridges using a component-level cost estimation approach, *Earthquake Engng Struct. Dyn.* 40: 1743–1761.

[65] Proske, D. and Curbach, M. (2005), Risk to Historical Bridges Due to Ship Impact on German Inland Waterways, *Reliability Engineering and System Safety,* 90(2–3): 261–270.

[66] AP (2009), Pakistan Militant Attack Cut US, NATO Supply Line for Afghanistan, *Associated Press,* 3 February 2009.