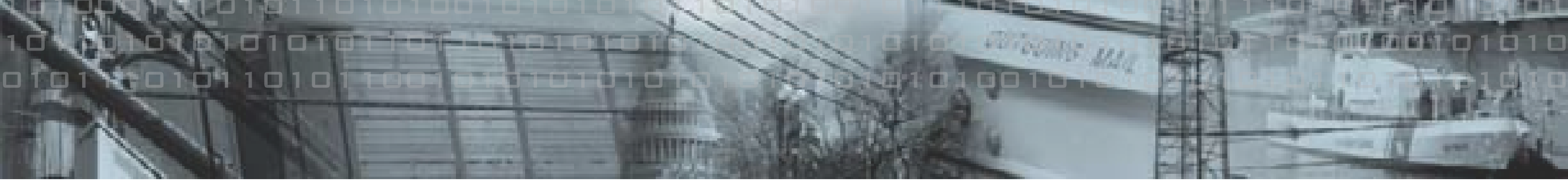

THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 10 NUMBER 5

NOVEMBER 2011

RISK MANAGEMENT

EDITORIAL STAFF

EDITORS
Devon Hardy
Olivia Pacheco

STAFF WRITERS
M. Hasan Aijaz
Shahin Saloom

JMU COORDINATORS
Ken Newbold
John Noftsinger

PUBLISHER
Liz Hale-Salice

Contact: dhardy1@gmu.edu
703.993.8591

Click here to subscribe. Visit us online
for this and other issues at
http://cip.gmu.edu

GEORGE MASON UNIVERSITY
School of Law
CENTER
for
INFRASTRUCTURE PROTECTION
and
HOMELAND SECURITY

This month's issue of *The CIP Report* focuses on risk management. In particular, we highlight the link between infrastructure protection and risk management.

First, the U.S. Department of Homeland Security (DHS) discusses the Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI), a new effort launched by DHS to strengthen infrastructure protection and resilience across all sectors and regions. The risks, costs, and benefits of counter-terrorism protective measures for infrastructure is then assessed by the Director of the Centre for Infrastructure Performance and Reliability at The University of Newcastle, Australia and Professor and Woody Hayes Chair of National Security Studies at Ohio State University. Next, the L.Q. Professor of Engineering and Applied Science at the University of Virginia examines the vulnerabilities and resilience of infrastructure systems. A Senior Expert on Risk Management at the European Network and Information Security Agency (ENISA) then provides an overview of the link between national risk management preparedness and critical information infrastructure protection. The President of the Security Analysis and Risk Management Association (SARMA) explains the benefits of a risk-based approach to managing the Federal Emergency Management Association's (FEMA) preparedness grants. An Associate Professor in the Department of Civil and Environmental Engineering at the University of Delaware then provides insights into the new concept of Resilience Engineering. The future of infrastructure protection is then considered by a doctoral student in the Department of Computer and Telecommunications Systems at the University of Florence and a representave from the European Commission's Joint Research Centre, Institute for the Protection and Security of the Citizen, Security Technology Assessment Unit. Finally, an Associate Professor of Law at the University of Colorado Law School reviews the history of the Terrorism Risk Insurance Act of 2002.

This month's *Legal Insights* analyzes the role of the Legal Risk Manager in protecting critical infrastructure.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Assessing the Risks, Costs, and Benefits of Counter-Terrorism Protective Measures for Infrastructure

by Mark G. Stewart and John Mueller*

Evaluating protection measures and policies in a responsible manner does not simply involve ranking targets by their vulnerabilities, by the consequences of an attack on them, or by the likelihood they will be attacked. Rather, it requires a composite cost-benefit assessment in which the costs of protection are systematically blended with the consequences of an attack on a target, with the likelihood the target will be attacked, and the degree to which protection reduces the consequences and/or the likelihood of an attack, keeping in mind issues like the potential for displacement or risk transfer.

The *benefit of a security measure* is a function of three elements:

> Benefit = (probability of a successful attack) × (losses sustained in the successful attack) × (reduction in risk)

The *probability of a successful attack* is the likelihood a successful terrorist attack will take place if the security measure were not in place. The *losses sustained in the successful attack* include the fatalities and other damage — both direct and indirect — that will accrue as a result of a successful terrorist attack. The *reduction in risk* is the degree to which the security measures foil, deter, disrupt, or protect against a terrorist attack. This *benefit*, a multiplicative composite of three considerations, is then compared with the costs of providing the risk-reducing security required to attain the benefit.

The same equation can be used in a break-even analysis to calculate how many attacks would have to take place to justify the expenditure:

> Probability of a successful attack = security cost/ [(losses sustained in the successful attack) × (reduction in risk)][1]

Many reports and studies have highlighted the vulnerability of critical infrastructure to terrorism, and the list of potential targets is extensive, typically including buildings, bridges, airports, dams, pipelines, ports, and nuclear facilities. This article focuses on bridges and applies break-even cost-benefit analysis to determine the minimum probability of a successful attack, absent the security measures, that is required for the benefit of the security measures to equal their cost.

There are 600,000 highway bridges in the United States. Moreover, bridges are — or seem to be — especially vulnerable. It happens, however, that a bridge is very difficult to damage severely because its concrete and steel construction makes it something of a hardened structure from the outset. Buildings are far more vulnerable, and many casualties can be caused if their thin and brittle masonry and glass facades are shattered. 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 that 10 perished in any single attack (See Figure 1 on Page 4).

Since highway bridges have a large variety of spans, widths, geometry, and other characteristics, it is difficult to generalize about damage costs. However, the replacement and demolition costs for two damaged U.S. interstate highway bridges were $4 million and $11.75 million, and for bridges in Los Angeles from $6.2 million to more than $60 million. Applying this experience, we set replacement costs for a typical interstate highway bridge at $20 million. In addition to the economic cost of traffic diversion, there are other social and economic costs to a community. These are

(Continued on Page 4)

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

Counter-Terrorism *(Cont. from 3)*

harder to quantify but may be in the order of tens to hundreds of millions of dollars because loss of one bridge 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 20, at a cost of $130 million based on value of statistical life considerations.[2] The total losses for a damaged bridge, including both the loss of life and economic considerations, thus come approximately to $250 million. This, then, would be the *losses sustained in a successful attack* element in the break-even equation above.

Table 1: The probability of an otherwise successful terrorist attack, in percentage per year, required for protective security expenditures to be cost-effective, assuming the expenditures reduce the risk of an attack by 95 percent. Note: A probability greater than 100 percent denotes more than one attack per year.

Cost of security measures (per year)	Losses from a Successful Terrorist Attack						
	$10 million	$100 million	$250 million	$1 billion	$2 billion	$10 billion	$100 billion
$1,000	0.01	0.001	0.0004	0.0001	0.00005	0.00001	0.000001
$100,000	1.0	0.1	0.04	0.011	0.005	0.001	0.0001
$250,000	2.6	0.3	0.11	0.026	0.013	0.003	0.0003
$500,000	5.3	0.6	0.21	0.053	0.026	0.005	0.0005
$1 million	10.5	1.1	0.42	0.105	0.053	0.011	0.0011
$5 million	52.6	5.3	2.10	0.526	0.263	0.053	0.0053
$10 million	105.3	10.5	4.20	1.050	0.526	0.105	0.0110
$100 million	1052.6	105.3	42.10	10.526	5.263	1.053	0.1060
$500 million	5263.2	526.3	210.50	52.650	26.316	5.263	0.5263

We will conservatively assume that substantial mitigation of blast effects can be achieved at a cost of 20 percent of a bridge's replacement value. If the bridge replacement value is $20 million, the cost of strengthening it is then $4 million. Annualized over a remaining service life of roughly 10 years, this comes to a present value cost of approximately $500,000 per year. This, then, would be the *security cost* element in the break-even equation above.

As for the *reduction in risk* element in that equation, we will generously assume that protective measures reduce the risk by 95 percent. This is substantial and biased in favor of showing that security measures are cost-effective.

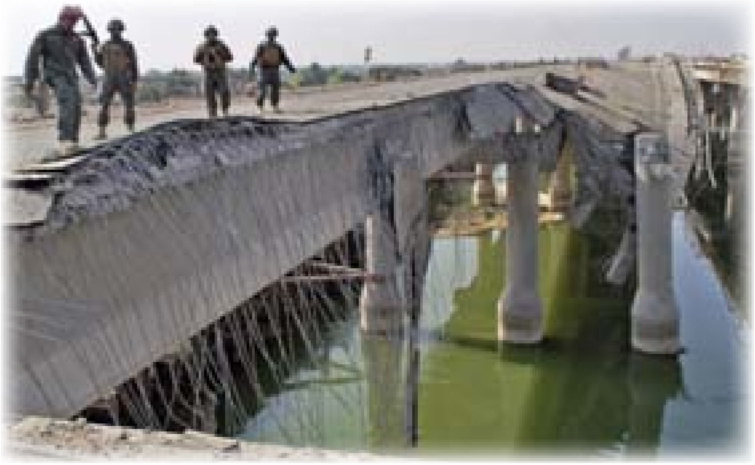

Figure 1: Vehicle Borne Improvised Explosive Device (VBIED) Damage to Bridge in Iraq (2009).

Table 1 arrays the annual attack probabilities required at a minimum for security expenditures on protecting a bridge to be cost-effective, assuming the expenditures reduce risk by an impressive 95 percent. This break-even analysis shows that protective measures that cost $500,000 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 0.21 percent or one in 480 per bridge per year.[3]

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 because there are

(Continued on Page 5)

[2] Value of statistical life is taken to be $6.5 per life saved (in 2010 dollars) as suggested by Lisa A. Robinson, James K. Hammitt, Joseph E. Aldy, Alan Krupnick, and Jennifer Baxter, "Valuing the Risk of Death from Terrorist Attacks," *Journal of Homeland Security and Emergency Management*, 7(1), (2010).

[3] If we assume risk is reduced only by 50 percent (not 95 percent), the minimum attack probability per year required for bridge protective measures to be considered cost-effective increases to 0.4 percent per bridge.

Counter-Terrorism *(Cont. from 4)*

600,000 bridges in the country. This probability is obviously nowhere near the 1 in 480 likelihood of a successful attack required for bridge protective measures to be cost-effective.

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

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," and that, summing reconstruction costs and socioeconomic losses, the "loss of a critical bridge or tunnel could exceed $10 billion."[4] This is certainly alarming, and 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 million to more than $157.4 million. The protection costs include strengthening (retrofitting) piers, anchors, road deck, tension hangars, and approach highways. These are enormous protective costs. 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 (see page 4). Applying the panel's dire expected losses of $10 billion with protective costs rounded down to $5 million per year, the attack probability would need to exceed 0.05 percent, 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.

Nearly half of American Federal homeland security expenditure is devoted to protecting critical infrastructure and key resources. Applying commonsense English about what critical infrastructure could be taken to mean, it should be an empty category. If any element in the infrastructure is truly "critical" to the operation of the country, steps should be taken immediately to provide redundancies or backup systems so that it is no longer so. Also, key resources are defined to be those that are "essential to the minimal operations of the economy or government." It is difficult to imagine what a terrorist group armed with anything less than a massive thermonuclear arsenal could do to hamper such "minimal operations." The terrorist attacks of 9/11 were by far the most damaging in history, yet, even though several major commercial buildings were demolished, both the economy and government continued to function at considerably above the minimal level.

Furthermore, it appears that vast sums of money are spent under the program to protect elements of the infrastructure whose incapacitation would scarcely be debilitating and would at most impose minor inconvenience and quite limited costs and would scarcely hamper the minimal operations of the economy or government.

There is no doubt that a terrorist attack on many infrastructure elements could cause considerable damage and significant loss of life. However, while targets such as buildings, bridges, highways, pipelines, mass transit, water supplies, and communications may be essential to the economy and well-being of a society, damage to one or even several of these, with few exceptions, will not be "critical" to the economy, or to the state.

In part, this is because infrastructure designers and operators place much effort on systems modeling to ensure that a failure of one node will not keep the network from operating, even if at reduced efficiency. This is done routinely. For example, it is necessary to close

(Continued on Page 31)

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

Counter-Terrorism *(Cont. from 5)*

many bridges from time to time for maintenance or repair, and therefore traffic is redirected so that the network is not interrupted. Other failures routinely planned for include traffic accidents, severe weather, earthquakes, and equipment malfunctions. In other words, as a matter of course, infrastructure is designed with built-in redundancies and backup systems to ensure resilience in the event of anticipated or unexpected hazards.

There is also a displacement effect, a transfer of risk. Terrorists can choose, and change, their targets, depending on local and immediate circumstances. If the protection of one target merely causes the terrorist to seek out another from among the near-infinite set at hand, it is not clear how society has gained by expending effort and treasure to protect the first.

Relying on standard evaluative measures accepted for decades by analysts, governments, regulators, and risk managers, our analyses suggest, then, that bridges require no protective measures unless, perhaps, there is a very specific threat to them.[5] The same, it is likely, applies to many other individual items of infrastructure. ❖

For additional and wider-ranging assessments of the issues raised and the approaches used, see John Mueller and Mark G. Stewart, *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security*, New York and Oxford, UK: Oxford University Press, September 2011.

For more information, please contact the authors at:

Mark G. Stewart
Australian Research Council Professorial Fellow and Professor of Civil Engineering
Director, Centre for Infrastructure Performance and Reliability
The University of Newcastle, New South Wales, Australia
+61 2 49216027
mark.stewart@newcastle.edu.au
www.newcastle.edu.au/research-centre/cipar/staff/mark-stewart.html.

Professor Mark Stewart is Director of the Centre for Infrastructure Performance and Reliability at The University of Newcastle, and Professor John Mueller holds the Woody Hayes Chair of National Security Studies at Ohio State University. Their book, <u>Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security</u>, has recently been published by Oxford University Press and will be available in Australia by October.

John Mueller
Professor and Woody Hayes Chair of National Security Studies
Mershon Center for International Security Studies and Department of Political Science Ohio State University, Columbus, Ohio 43201
USA
+1 614 247-6007
bbbb@osu.edu
polisci.osu.edu/faculty/jmueller

[5] It might also be noted that 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.