What Price Security?

Donald C. Masters
Board of the Homeland Security Innovation Association (HLSIA), masters@hlsia.org

What Price Security?

Abstract

This article presents a critique of the Copenhagen Consensus Center's(CCC) exhaustive study on transnational terrorism, published in 2008.The implications of this study are controversial, yet highly relevant in today's economic environment. The Obama administration must come toterms with fiscal realities that will challenge budget priorities and invigorate what will undoubtedly prove to be tough negotiations on Capitol Hill for homeland security dollars. It is proposed here that standard economic tools such as benefit cost analysis, cost effectiveness criteria, and simulation models can help identify areas where security can be either extended or improved using fewer resources. Greater movement towards competitive procurement practices will also result in lower costs and higher returns on security investments.

What Price Security?

By Donald C. Masters, Ph.D.

Introduction

This article presents a critique of the Copenhagen Consensus Center's (CCC) exhaustive study on transnational terrorism, published in 2008. The implications of this study are controversial, yet highly relevant in today's economic environment. The Obama administration must come to terms with fiscal realities that will challenge budget priorities and invigorate what will undoubtedly prove to be tough negotiations on Capitol Hill for homeland security dollars. It is proposed here that standard economic tools such as *benefit cost analysis*, *cost effectiveness criteria*, and *simulation models* can help identify areas where security can be either extended or improved using fewer resources. Greater movement towards *competitive procurement* practices will also result in lower costs and higher returns on security investments.

The Copenhagen Study

For this study, the Copenhagen Center commissioned two academic economists, Todd Sandler and Walter Enders of the Universities of Texas and Alabama respectively, to evaluate the human costs and economic consequences of terrorism in conjunction with government expenditures on anti-terrorism efforts.[1] The study's objective was to quantify the benefits of (a) lives saved and injuries avoided and (b) economic losses averted compared to the budgetary costs associated with homeland security. Their research uses standard benefit-cost methodology to calculate the estimated *return on investment* compared to alternative "solutions."

The study deals only with "transnational" terrorism, defined as terrorist activity that crosses international borders as opposed to domestic insurgencies or resistance to foreign occupation. They observe that "terrorism is a tactic of asymmetric conflict, deployed by the weak for strategic advantage against a strong opponent." In their view, there is no permanent solution to transnational terrorism because it is a cost effective tactic. Their analysis of international trends related to terrorist incidents found that on average 420 people are killed and 1,249 are injured annually.[2] Yet, guarding against terrorism can consume resources at an alarming rate without a permanent reduction in terrorist activity.

33

Obviously, an international study of this complexity requires some heroic assumptions regarding the relative magnitudes of benefits and costs. By and large, the authors are explicit in stating their underlying assumptions and conducted extensive sensitivity analysis to determine the reasonableness of their estimates. Where reasonable doubt exists they took the optimistic scenario favoring higher benefits or lower costs. The data for the main variables driving benefits and costs were estimated from a number of studies or drawn from official budgets and national income accounts.

Benefit Cost Ratios

Benefit cost ratios (BCR) are one method for calculating the net discounted return on investment. The BCR is a discounted ratio of benefits to costs. It is similar to the more familiar *present value* approach, which subtracts discounted costs from benefits to show net return. Accordingly, the present value method provides an absolute dollar value while BCR is a ratio expressed in decimal form. The *investment rule* (for both) is to make the investment if either is greater than one, assuming full access to capital resources. If resources are constrained (the normal situation) then either method can be used to rank order *alternative* investments from highest ranked investment down to the investment that exhausts available capital resources. When there is lack of certainty regarding the benefits and costs over time, then the BCR method takes on characteristics similar to a probabilistic decision model. In other words, the BCR approach estimates an order of magnitude based on a range of values for key variables driving the analysis.

In the Copenhagen study, three key variables are identified as determining benefits and costs. They are: (1) fatalities and injuries sustained in terrorist attacks, (2) Gross Domestic Product (GDP) losses associated with destruction or disruption of economic activity, and (3) security costs to governments in countering terrorist threats. Although all three are calculated as "costs" either to terrorism victims or their governments, the first two are treated as benefits that would accrue if *government anti-terrorist programs cause these losses to be averted*. Alternatively stated, the benefit cost approach compares terrorism losses to society that would have occurred if governments did *not* undertake security measures to protect their citizens. In the arcane language of the economist, the benefit cost approach estimates a *counterfactual* of what would have occurred in the absence of investments in security measures. In this manner, net benefits and costs can be compared when appropriately discounted over a period of time. In this study, five-year capitalized values were used for both benefits and costs. Briefly, the key variables are as follows:

34

Benefits

Available data were assembled to show average annual casualties in terms of deaths and injuries due to terrorist acts. The fatalities were valued in terms of life expectancies at the time of death and compensation paid to families. The injuries were categorized by type and severity in order to estimate their weighted distribution and corresponding disability costs. This weighted cost formula was derived from a French study that used time series data for fatalities and injuries associated with a typical terrorist incident. Thus, the number of fatalities along with the associated (weighted distribution) injuries could be "priced" to show the dollar value of benefit of an averted terrorist attack attributable to enhanced homeland security. The variable estimated could then be adjusted to reflect higher or lower death compensation and disability values by region and average per capita income.

Since terrorism destroys property and/or disrupts economic activity, an estimate of economic costs was also calculated. The authors used estimates provided in a 2004 study that calculated the economic losses in terms of forgone economic growth on a per capita basis. The estimates were then applied to countries that experienced transnational terrorism over the period 2001–2005. The data sources for this calculation came from country national income accounts. For example, the GDP loss due to foregone growth over a five-year period, for some seventy countries, amounted to $83 billion. Of this amount, the United States had the highest GDP loss calculation at an estimated $37 billion.[3]

Costs

The authors relied heavily on public expenditure data from the United States and Britain since they (1) represented the main country targets of transnational terrorism and (2) their budget data were the most explicit regarding security costs since 9/11. There was a high cost estimate for "proactive" anti-terrorism efforts, which included both domestic and overseas costs associated with the invasions of Iraq and Afghanistan. These costs were converted into a percent of GDP for the base year 2005. The lower cost estimate for purely "defensive" homeland security efforts was similarly calculated. In the end, the authors used the lower "defensive" cost estimates combined with a lower proxy estimate for the 66 countries that experienced terrorist acts but were not considered main target countries.[4]

35

Journal of Strategic Security

Analysis Results

The calculated benefit cost ratios (BCRs) ranged from a low of 0.039 to a high of 0.095 depending on alternative assumptions. This range is surprisingly low, showing a *return on security investments of less than ten cents on the dollar*. Nevertheless, the calculations are viewed as "robust" in light of the data sources and methodologies used.

Alternative "Solutions"

Some of the solutions showing less adverse BCRs are briefly outlined below:

- Greater International Cooperation—Freezing terrorists' financial assets would reduce funding available to launch attacks, while greater extradition of suspected terrorists for prosecution might also reduce their organizational capacity. Both would require greater international cooperation which, if achieved, would be a low cost option. The stepped up monitoring of financial transfers and remittances could be implemented by the International Monetary Fund, working in tandem with member country central banks and regulators. The proposed doubling of the Interpol budget from $58 million to $116 million would help improve international police coordination in apprehending and extraditing suspected terrorists. It was noted that this solution would not impact on small "routine" attacks but would make larger scale "spectacular" attacks less likely; thereby saving a considerable number of lives and property. The BCR ranged from 5.348 to 15.504, giving this approach the highest return on investment.

- Augmented Defensive Measures—Better border security and hardening of critical infrastructure as well as public safety measures raise costs but might result in 25% fewer successful attacks. However, it was noted that there would likely be some *transference* to softer targets. Countries taking this approach might well assign a higher compensation value thereby raising calculated benefits. Accordingly, the estimated BCRs range from 0.281 to 0.304 which are still adverse and (in the opinion of the authors) not likely to change significantly with additional resources dedicated to defensive measures.

General Observations

Clearly the study represents an ambitious effort. While it is possible to question some of the techniques used to derive the cost estimates, it is

evident that costs tend to overwhelm benefits. This causes the BCRs to fall short of the investment breakeven point. At the margin, governments can and should seek lower-cost countermeasures while anticipating more lethal threats in the future. Although there was some discussion of chemical, biological, and radiological/nuclear (CBRN) weapons eventually finding their way into terrorist hands, there was no attempt to model this eventuality into their benefit cost framework. Rather they suggest that there are "inhibitors" that make it unlikely that terrorists will increase their lethal capabilities in the foreseeable future.[5] This may be an unrealistic assumption. A "rogue" state possessing CBRN weapons might collude with terrorists, providing them with the means of inflicting far greater casualties and economic loss. Even in the absence of such collusion between a "state actor" and a "non-state actor," a biological weapon could be developed by terrorists in the near future.[6] Such a scenario would shift the benefit stream considerably upwards, yielding a significantly higher BCR. This would certainly be a "game changer" and well worth considering in greater detail.

Benefit cost analysis is most usefully applied *within the same* organizational unit responsible for budget planning and program design. The U.S. Department of Homeland Security (DHS) would be, in this context, the relevant entity with independent oversight provided by the Government Accountability Office (GAO). For public goods, such as *security*, it is often more difficult to value benefits than measure financial costs. For this reason, it is sometimes helpful to develop measurable indicators that correlate closely with intended benefits. This requires metrics that meaningfully represent improved security, such that *cost effectiveness* becomes the operational measure of efficiency. For example, a security program might call for the protection of critical infrastructure with security measures designed to "harden" a facility from a possible terrorist threat. The task can be defined as selecting security systems that are most cost effective in reducing the probability of a successful attack. If a security output can be measurably defined, then we are simply looking for the least expensive combination of systems, i.e. equipment and personnel (inputs) to attain a given level of security (output).

Port security would be an example. The security threat involves the smuggling of illicit or dangerous materials in intermodal shipping containers. The primary threat would be a bomb of some kind in which the port itself or some inland destination may be the intended target. The security mission is to maintain normal port operations while identifying (and disposing of, if necessary) containers that pose a serious threat. The procurement and deployment task is to do this at least cost.

37

Journal of Strategic Security

Layered Security Systems: Redundant Costs?

The concept of layered security is to create a dense protective shield that reduces the risk of a successful terrorist attack. The layered security approach is often applied to critical infrastructure. However, without an overall measure of facility protection, security "layers" and their associated costs may be unnecessarily added over time.

Conditional probability theory lends some support to this approach, but only if certain conditions are met. To illustrate, assume there are three security systems that use older technology that is only 50% effective in preventing an attack. In this example, each system probability (p) is set equal to 0.50 yielding an effectiveness rate similar to the random flipping of a coin. However, when *all* three systems are used in concert the resulting vulnerability declines markedly, as shown below:

$$(0.50) \text{ x } (0.50) \text{ x } (0.50) = 0.125$$

This yields a 1:8 probability of a successful attack on the facility. This probabilistic measure of vulnerability could be further reduced if (a) additional layers and corresponding probabilities were added and/or (b) better security technologies with higher probabilities of prevention were substituted for older systems. Importantly, this approach assumes that each component system is independent or operates autonomously, such that defeating one system does not affect the others. The other condition is that none of the systems can be circumvented by the attacker. (Some well-known examples of circumvention include the Trojan Horse and, in modern times, the Maginot Line).

Taking this illustration further in the context of port security, assume we have three systems (Advanced Spectroscopic Portals–ASP, Automated Targeting System–ATS, and Hazmat) which together provide detection capability against an explosive device, either conventional or radiological/ nuclear. The ASP system relies on different technologies jointly deployed amounting to a two-tier scanning process.[7] This newer technology costs more than five times as much as existing technology. A cost benefit analysis of the two types of scanning equipment was performed but the results were inconclusive at the time.[8]

Nevertheless, for the purpose of this example, assume that an optimal technical ratio or deployment configuration has been established, such that the operation of the primary scanning system, which is a polyvinyl toluene (PVT)-based gamma-ray scintillation detector, is fully coordinated with the more expensive ASP secondary scanners. The result is a

38

combined effectiveness probability of, say, 90%. Similarly, we assign differing successful attack probabilities for each of the three systems, shown below. The first involves analysis of electronic manifests (ATS) and the assignment of container risk scores; second, a two-tier scanning system (ASP) and, third, a countermeasure procedure to deal with "positive" detections (Hazmat). Hence, the port security "architecture" could be summarized as follows where the numbers in parentheses represent probabilities of successful detection for each system:

ATS (0.80) x ASP (0.10) x Hazmat (0.25) = 0.020 probability of success

The conditional probability (P) derived from this simple equation suggests that an attack would have only a 1:50 or 2% chance of success. This implies that the port is now 98% secured from bomb threats. At this level of security, additional "layers" may not be warranted given their associated costs. However, if a rare (P = 0.020) but potentially high consequence event occurs, then *mitigation strategies* may be more cost effective. To determine this in economic terms, we draw on insurance theory and the concept of *expected value of an outcome*. This is calculated as the product of the probability and the value-at-risk of the asset. This dollar amount determines the risk premium to be paid. If the port facility suffered a billion dollar loss then the annual premium would be $20 million. Given that more than 10 million containers arrive at U.S. ports every year, a fee of $2 per container would cover this premium. Thus, an optimal port strategy might use *protective and mitigation strategies* together, if this translates into greater cost efficiency.

Systems Analysis and Cost Minimization

Models can simulate system operations to help identify and estimate security *compliance costs* borne by the private sector. Several years ago, Sandia National Laboratories, drawing on Seattle-Tacoma port data, designed a simulation model to evaluate the impact of port security initiatives on container operations.[9] A team representing experts and stakeholders pooled information to systematically estimate short- and long-term impacts. The resulting port "system dynamics" model estimated short-term effects of increased security on (a) shipping cost and (b) delivery time. In addition, the model estimated the port's longer term competitive prospects related to increased costs of security measures. They concluded that the implementation of security measures in a piecemeal fashion had competitive disadvantages for "early adopter" ports. The simulation took into account the high fixed costs of port operations and the limited cost recovery attainable by raising port charges. In a competi-

39

tive market, individual ports cannot easily pass on security costs to carriers since this could divert shipping traffic. The related loss in container volumes creates a dynamic leading to a downward "revenue" spiral that could ultimately threaten port commercial viability.

Sandia's simulation exercise suggests that security enhancements should take into account their effects on commercial operations. Even though equipment costs may be borne by the government, at least initially the localized impact on port operations may generate significant private costs. One approach for planned rollouts of new security measures would be the development of a "generic" port model. This could identify the main parameters that influence trade flows and operational costs, which could then be built-out or "customized" for specific port conditions. This might include the number of loading and stacking cranes available; container ship berths and schedules; and container storage areas linked to onward transportation facilities. The flow of containers per unit of time (or "throughput") could be estimated given infrastructure constraints and security requirements. The *constrained optimization problem* would be to minimize time delays and associated costs while achieving a predetermined level of port security.

Procurement Reform

The search for "economies" with respect to homeland security will inevitably turn to procurement. The ability of DHS to secure favorable prices from suppliers and contractors is critical given the magnitudes involved. The value of contracts awarded by the DHS claimed one-third of budget resources in fiscal years 2006–2008. This amounted to approximately $40 billion over a three-year period. Moreover, DHS grants to state and local institutions create cascading procurements that have substantial resource allocation implications. The *Federal Acquisition Act*, as amended, formally enshrines "competition" as the guiding principle for all government procurements. Following 9/11, Congress gave DHS extensive procurement authorities as well as multi-year program funding. This included "other" procurement methods (non-competitive) to expedite the nation's defenses to counter expected terrorist attacks. As a consequence, large multi-year contracts were awarded on a non-competitive basis, usually justified by the determination that only one firm had "predominant capability" in a certain technical area.

As late as fiscal year 2006, roughly 39% of all federal contracts fell into the category "not competed for an allowable reason."[10] In more recent years, there has been movement towards less prescribed contracting prac-

40

tices. Nevertheless, the category "competed but only one bid was received," suggests a lack of *effective competition*. Combining these two categories gives a ratio of non-competitive to competitive awards of roughly two to one. Overall, 50% of all DHS procurements between fiscal years 2006–2008 were *less* than fully competitive. Economists generally agree that competition provides the lowest prices, thereby mobilizing the most resources from a given budget. Thus, an indicator of procurement reform would be contract awards gradually becoming more competitive.

The deployment of new advanced technologies poses the most difficulty to procurement reforms since (by definition) they do not have exact bid specifications or "off the shelf" equivalents. For this reason, grant funding is often used for applied research and development of prototypes. However, technologically sophisticated contracts have been awarded for large-scale projects. Various GAO reports suggest that the procurement methods, including contract management at the implementation stage, have proved problematic in certain cases. Well known indicators include significant project delays and related cost overruns. These projects are technology intensive and often complex, requiring exceptional management oversight. The latter cannot easily be "contracted out" as this sometimes poses conflicts of interest. On balance, DHS may have to consider a number of options that will increase internal administrative costs. One would be the development of a *technical cadre* to serve as program managers. Another option would be to hire and train additional *procurement officers* to handle the increased workload related to smaller "bite size" contracts. These would be more labor-intensive to compete but would encourage greater medium-size firm participation. Firms in this size category may prove more adept at designing and implementing less costly security systems.

Conclusion

Projected U.S. Government deficits will likely create a constrained fiscal environment in the years ahead. Barring another high profile terrorist attack on American soil, homeland security may become less of a budget priority. Coming to terms with the new fiscal realities will be a major challenge for senior management. We have suggested here that standard economic tools such as *benefit cost analysis*, *cost effectiveness criteria*, and *simulation models* can help identify areas where security can be either extended or improved using fewer resources. Greater movement towards competitive procurement practices will also result in lower costs and higher returns on security investments.

41

Journal of Strategic Security

About the Author

Donald C. Masters, Ph.D., was formerly with the International Bank for Reconstruction and Development (1973–1975) in the Public and Private Finance Division. He subsequently joined the U.S. Foreign Service (1977–97) where he advised governments on economic and fiscal policies. During rotations at the State Department, he served as USAID Officer-in-Charge for various countries including Morocco, Tunisia, and Jordan. In 1998, he became a senior consultant for the International Development Business Consultants (IDBC) and later joined the faculty at the Monterey Institute of International Studies as an Adjunct Professor of Economics (1999–2002). Currently, he is an Executive Director on the Board of the Homeland Security Innovation Association (HLSIA), a private non-profit corporation whose primary mission is to aggregate information, disseminate potential solutions, and articulate technology-related issues pertinent to homeland security. Dr. Masters can be reached for comment at: *masters@hlsia.org*.

References

1 "Terrorism," *Copenhagen Consensus 2008 Challenge Paper*, February 2008, available at: *http://www.copenhagenconsensus.com/Default.aspx?ID=1152*.

2 Ibid, "Transnational Terrorism," *Executive Summary*, see Table 2.

3 Ibid, Table 12.

4 Ibid, Table 11.

5 Ibid, pp.56–57.

6 Bob Graham et al., *World at Risk: Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism* (New York: Vintage Books, 2008).

7 For more information, see "Combating Nuclear Smuggling: DHS' Program to Procure and Deploy Advanced Radiation Detection Portal Monitors is Likely to Exceed the Cost Estimates," *Government Accountability Office*, GAO-08-1108R, September 22, 2008, available at: *http://www.gao.gov/products/GAO-08-1108R*.

8 For details of cost benefit analysis results, see "Combating Nuclear Smuggling: DHS' Decision to Procure and Deploy the Next Generation of Radiation Detection Equipment is Not Supported by its Cost Benefit Analysis," *Government Accountability Office*, GAO-07-581T, March 14, 2007, available at: *http://www.gao.gov/products/GAO-07-581T*.

9 Thomas Corbet et al, "Evaluating the Economic Impact of Port Security Initiatives on Container Operations," *National Infrastructure Simulation & Analysis Center* (Monograph, Sandia National Laboratories, 2005).

10 See *http://www.usaspending.gov* for federal contract award statistics.

42