

Evaluating Counterterrorism Spending

John Mueller and Mark G. Stewart

In 2010, a committee of the National Research Council of the National Academies of Science issued a report on how effectively the Department of Homeland Security (DHS) was spending its funds. The committee praised the approaches used in the department for decisions about natural hazards, saying they were “near state of the art . . . based on extensive data, have been validated empirically, and appear well suited to near-term decision needs.” In contrast, with regard to the department’s spending on counterterrorism, the committee could “not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making” and observed that “little effective attention was paid to the features of the risk problem that are fundamental” (National Research Council 2010). As far as we can tell, this seemingly newsworthy report inspired no media coverage whatever.

In general, it seems, counterterrorism agencies simply identify a potential source of harm and try to do something about it, rather than systematically thinking about the likely magnitude of harm caused by a successful terrorist attack, the probability of that attack occurring, and the amount of risk reduction that can be expected from counterterrorism efforts. Without considering such factors, it is impossible to evaluate whether security measures reduce risk sufficiently to justify their costs.

■ *John Mueller is Senior Research Scientist, Mershon Center for International Security Studies and Adjunct Professor of Political Science, both at Ohio State University, Columbus, Ohio. He is also a Senior Fellow, Cato Institute, Washington, DC. Mark G. Stewart is Australian Research Council Professorial Fellow and Professor and Director, Centre for Infrastructure Performance and Reliability, both at the University of Newcastle, New South Wales, Australia. Their email addresses are bbb@osu.edu and mark.stewart@newcastle.edu.au, respectively.*

In this article, we lay out a simple, back-of-the-envelope approach for evaluating counterterrorism spending that uses only four variables: the consequences of a successful attack, the likelihood of a successful attack, the degree to which the security measure reduces risk, and the cost of the security measure. After measuring the cost of a counterterrorism measure, we explore a range of outcomes for the costs of terrorist attacks and a range of possible estimates for how much risk might be reduced by the measure. Then working from this mix of information and assumptions, we can calculate how many terrorist attacks (and of what size) would need to be averted to justify the cost of the counterterrorism measure in narrow cost–benefit terms.

To illustrate this approach, we first apply it to the overall increases in domestic counterterrorism expenditures that have taken place since the terrorist attacks of September 11, 2001, and alternatively we apply it to just the FBI’s counterterrorism efforts. We then evaluate evidence on the number and size of terrorist attacks that have actually been averted or might have been averted since 9/11. We also consider the degree to which our conclusions would be altered if we believe deaths from terrorist attacks should be given greater weight than deaths caused by hazards like natural disasters or traffic accidents.

Assessing Increases in Domestic Counterterrorism Expenditures since 9/11

Our evaluation of the rise in domestic counterterrorism expenditures relies on three main ingredients: how much such expenditures have in fact increased; the range of possible costs of terrorist actions; and the risk reduction from the increase in counterterrorism expenditures. Based on these three factors, we can calculate how many terrorist attacks would have had to be averted for the rise in counterterrorism spending since 9/11 to be justified. From this calculation, it appears likely that the rise in counterterrorism spending was too large.

By our calculation, domestic counterterrorism expenditures per year were about \$25 billion in 2010 dollars before the terrorist attacks of September 11, 2001. These increased by about \$75 billion in the subsequent decade or so. Spending on homeland security by the Department of Homeland Security, the Department of Defense, the Department of Justice, the Department of Health and Human Services, the Department of Energy, and 26 other such federal agencies was \$50 billion more in 2010 dollars than in 2001, adjusting for inflation. To this we add the costs of US intelligence focused on the homeland. Overall intelligence operations were \$80 billion in 2010. A core function is “protecting against the threat of international terrorism in the United States,” and we conservatively estimate increased intelligence expenditures since 9/11 devoted to domestic homeland security to be \$15 billion in 2010. Finally, enhanced outlays for state and local homeland security spending are approximately \$10 billion per year.

Although we will use this figure of \$75 billion per year for the annual increase in spending on domestic counterterrorism, it should be viewed as a very conservative

Table 1

How Many Terrorist Attacks Would Need to Occur Each Year in the Absence of All Counterterrorism Measures in Order to Begin to Justify a Counterterrorism Expenditure of \$75 Billion

	<i>Type of terrorist attack</i>					
	<i>Ft. Hood Shooting</i>	<i>Boston, Times Square bombing</i>	<i>London bombing</i>	<i>9/11</i>	<i>Nuclear bomb, port</i>	<i>Nuclear bomb, Grand Central Station</i>
Losses per incident	\$100 million	\$500 million	\$5 billion	\$200 billion	\$1 trillion	\$5 trillion
Level of risk reduction assumed						
10 percent	7,500	1500	150	4	.75	.15
25 percent	3,000	600	60	2	.30	.06
50 percent	1,500	300	30	.75	.15	.03
75 percent	1,000	200	20	.50	.10	.02
90 percent	833	167	17	.42	.08	.02
100 percent	750	150	15	.38	.08	.02

Notes: If the \$75 billion expenditure is expected to reduce the risk (the likelihood of, and/or the damage caused by, a successful terrorist attack) by 50 percent, those expenditures would need to deter, disrupt, or protect against at least half of the attacks in each entry in the 50 percent line. For the boxed entries, that would be 150 Boston-type attacks per year, 15 London-type attacks each year, or one 9/11-type attack about every three years.

measure of the degree to which homeland security expenditures have risen since 9/11. It leaves out nearly \$50 billion in various opportunity costs, like time spent in airports in security lines, as well as privacy issues and \$10 billion in costs incurred by the private sector (Mueller and Stewart 2011, pp. 81–82).

For thinking about the possible costs—both direct and indirect—inflicted by a terrorist attack, we lay out a range of possibilities across the top of Table 1. Deaths at the hands of terrorists are very often taken to be far more significant than those from other causes. Indeed, a study commissioned by the Department of Homeland Security suggests that, although human life is often taken to have a value of some \$6–\$7 million, lives lost to terrorism should be valued at twice that amount (Robinson, Hammitt, Aldy, Krupnick, and Baxter 2010). Others might suggest even higher multiples. In estimating the costs inflicted by a terrorist event, however, we prefer to value life at the more common figure, and then, on a case-by-case basis, we can discuss and add back in the indirect costs from economic, social, and psychological side-effects.

This approach can be illustrated by examining the attack costs arrayed in Table 1. Terrorism mostly inflicts losses that are quite low—in general, terrorism

is not only a low probability event, but also a low-consequence one, and the vast majority of terrorist attacks do not kill anyone (Mueller and Stewart 2011, chap. 3). However, at the low end of the scale in the table we start with events that impose a substantial loss of \$100 million. An example would be the shootings at Fort Hood in Texas in 2009 in which 13 people were killed. Although this has been by far the greatest loss of life inflicted in a terrorist act in the United States since 2001, almost all of the damage came in direct costs in the form of death and injury. It did not seem to cause additional substantial economic losses or widespread fear or anguish.

The direct and indirect losses inflicted in the Boston Marathon bombings of 2013 were probably much higher—in the vicinity of \$500 million—even though the death toll was lower. In addition to three deaths, hundreds of injuries, and property damage, the Boston terrorists inflicted considerable indirect losses on the region through the costs of pursuing them over the nearly four days they were on the loose. Travel to Boston was cancelled or deferred, and the large crime scene forced the closure of many businesses. The daily GDP for Boston is close to \$1 billion (Bureau of Economic Analysis 2013), so a reduction in economic activity of just 5 or 10 percent for several days represents a large sum. This amount might also be roughly the costs of the damage that would be inflicted at Times Square by a car bomb similar to the one a rather inept terrorist tried unsuccessfully to detonate there in 2010.

The losses sustained at the 2005 London and 2004 Madrid bombings that killed 52 and 191 commuters respectively are sometimes estimated to amount to \$5 billion in direct and indirect losses, with most estimates around \$2 or \$3 billion (for additional discussion of these estimates, see Mueller and Stewart 2011, chap. 3).

A number of studies have sought to assess the direct and indirect costs of the 9/11 terrorist attacks—far and away the most destructive single terrorist act in history and one in which the indirect costs considerably outweigh the (obviously horrific) direct ones. They generally conclude that a fair, if somewhat high, estimate for the full losses sustained in the attack—lives lost, property damaged or destroyed, psychological trauma, and indirect losses from travel and tourism reductions, business interruption, and economic shocks—would be some \$200 billion with loss of life valued at \$20 billion, direct physical damage at \$30 billion, and loss of GDP at \$70 to \$140 billion (equivalent to 0.5 to 1 percent of GDP) (as reviewed in Mueller and Stewart 2011, chap. 3). The potential losses if terrorists were able to set off an atomic bomb or device at an important port might reach \$1 trillion (Meade and Molander 2006). The losses for an atomic explosion at Grand Central Station in New York could be \$5 trillion (Bunn, Weir, and Holdren 2003), although the likelihood that terrorists could do this seems very small (Mueller 2010).

An additional consideration concerns what might be called extended (as opposed to indirect) costs. Thus, 9/11 not only led to considerable indirect costs as people avoided flying and traveling for a time, but the attacks also propelled the United States into expensive overseas wars (Stiglitz and Bilmes 2008). Few terrorist events trigger such extreme reactions, which can be considered either as contributors to the losses sustained in the terrorist attack or to the costs of counterterrorism.

We do not include such extended costs in the basic analysis here, but will return to this subject later in the discussion.

The rows of Table 1 show various degrees of risk reduction. In assessing risk reduction for increased security expenditures since 9/11, it is important to remember that a number of homeland security measures were already in place before that attack. In addition, the attacks of 9/11 massively heightened public awareness regarding the threat of terrorism, resulting in extra vigilance that has often resulted in the arrest of terrorists or the foiling of terrorist attempts. Most dramatically, airplane passengers rather than government counterterrorism efforts foiled the “shoe bomber” on a flight in December 2001 and the “underwear bomber” on a flight in December 2009.

In our analysis, we will assume that the security measures in place before 9/11 along with the extra vigilance of the public after that event combine to reduce risk by 45 percent. This estimate of risk reduction *not* associated with increased spending after 9/11 should be viewed as conservative. After all, the most cost-effective security measures are generally the first to be implemented. For example, a study of security measures in shopping centers found that the least costly measures, suspicious package reporting, reduced risk by 60 percent, but the costly and inconvenient searching of bags at entrances achieved only 15 percent risk reduction (LaTourrette, Howell, Mosher, and MacDonald 2006).

We will also assume that the increase in US expenditures on homeland security since 2001 has been dramatically effective at closing the gap. If the preexisting measures and the extra public vigilance reduce the risk by 45 percent, we will assume that the additional security expenditures put in place after 9/11 reduce the risk by another 50 percent. Thus the total risk reduction supplied by all the security measures is assumed to be 95 percent.

In Table 1, we evaluate the contribution of a security measure or set of measures which cost \$75 billion per year. The cells show the number of successful attacks per year that would be required to take place in the absence of all counterterrorism measures in order to begin to justify that expense (the breakeven point). This is shown for various attack scenarios and for various levels of risk reduction.

The boxed entries are for the assumption that \$75 billion in security expenditures reduces the risk of a terrorist attack (its consequences and/or its likelihood) by 50 percent. Under that assumption, in order for the costs of a \$75 billion security measure or set of security measures to begin to be justified, there would have to have been 300 attacks like the Boston bombing each year—or about one a day—in the absence of all security measures. Or 30 London-size attacks per year—more than one a week. Or about three 9/11 attacks every four years. To justify its expense, a security measure that reduces risk by 50 percent would be expected to deter, disrupt, or protect against half of these—the 300 Boston-type attacks per year would be reduced to 150, for example. In our case, that would be the task of the set of security measures added to those already in place in September 2001, while the existing security measures, combined with the added vigilance inspired by 9/11, would separately deter, disrupt, or protect against almost all of the rest.

Of course, one can also put together more complex mixtures of larger and smaller terrorist events, or tinker with the calculations of how much additional counterterrorism spending might reduce the risks. The approach applied here is designed to provide decision makers with a coherent perspective on the relevant parameters for counterterrorism expenditures and how they interact, but it does not of itself make the decision. The assumptions given here suggest that the increase of \$75 billion per year in counterterrorism spending has not been justified on a cost-effectiveness basis because such a justification requires that the risk has been reduced for an implausibly high number of terrorist operations. In a later section, we will consider various possible objections and qualifications for this conclusion.

Tables similar to Table 1 can easily be calculated for specific counterterrorism measures, some of which, such as hardened cockpit doors and the federal flight deck program (which allows pilots, flight engineers, and navigators to volunteer for training so that they can carry a firearm on flights), certainly appear cost-effective (Stewart and Mueller 2013b). Let's apply the same analytical framework to evaluate just the FBI counterterrorism spending on its own. The Bureau's highest priority since 9/11 has been to "prevent terrorism and promote the nation's security consistent with the rule of law," and it currently is involved in following up more than 5,000 terrorism tips—or, as they are known internally, "threats"—each day (Graff 2011, pp. 579, 398–99). Counterterrorism now accounts for close to \$3 billion of FBI expenditures while the budget for its criminal division is \$2.5 billion (Federal Bureau of Investigation 2013).

A table for a \$3 billion counterterrorism expenditure would be the same as Table 1 except that each entry would be divided by 25. We generously assume that by its efforts the FBI has succeeded in reducing the risks of a terrorist attack—that is, the consequences and/or the probability of an otherwise successful attack—by a full 90 percent. To justify its \$3 billion counterterrorism budget under that condition, the FBI spending alone would have to deter, disrupt, or protect against some six attacks of the size of the Boston Marathon attacks each year—one every two months. Alternatively, the FBI's efforts would need to reduce by 90 percent the effect of one or two London-type bombings every two years—some six or seven over the course of a decade. Or again alternatively, the FBI budget would justify itself by reducing by 90 percent a huge attack with direct and indirect damage equivalent to that inflicted by 9/11 once every 60 years. The assumption about risk reduction is quite significant: if the FBI's counterterrorism efforts only reduce the total risk of losses in a terrorist attack by 50 percent rather than 90 percent, the number of terrorist events that it would need to prevent or mitigate would nearly double.

Evaluating Prospective Terrorist Attacks in the United States

Up to this point, the discussion has not sought to discuss the actual likelihood or size of potential terrorist attacks in the United States. Instead, the analysis has worked backward from the size of counterterrorism budgets (building on assumptions about risk reduction) to infer how much damage from terrorist attacks would

need to be mitigated to justify the budget. But here, we tackle the question of the likelihood and size of prospective terrorist attacks in the United States. The underlying question is: are such attacks likely to be numerous and large enough to justify the size of the counterterrorism budget?

How Many Disclosed Terrorists?

Since September 11, 2001, 54 cases have come to light that involve Islamist terrorists who were either planning to commit, or actually did commit, violence within the United States (Mueller 2014). In the twelve years since the September 11 attacks, these terrorists have managed to kill 19 Americans, 16 of them with gunfire, and three with primitive homemade bombs. It is likely that, without counterterrorism spending, more of the plots would have reached fruition and caused damage, but it seems implausible that many of them would have resulted (for example) in \$500 million in damage. Some of the plots being hatched were relatively small-scale: for example, setting off a grenade in a trash bin in a mall or taking some potshots at a military recruitment center. Plotters in other cases did sometimes harbor visions of toppling large buildings, destroying airports, setting off dirty bombs, or bringing down the Brooklyn Bridge, but such visions seem to have been well beyond their actual capacities (Mueller and Stewart 2011, pp. 83–89; Mueller and Stewart 2012). Most other terrorists do not have as destructive an agenda as the Islamist ones (a notable exception from the years before 9/11 would be the Oklahoma City bombing in 1995), and so their inclusion would probably not change the general considerations of our analysis very much.

How Many Undisclosed Terrorists?

It is sometimes argued that there are many terrorist plots out there in addition to the ones that have entered the public record, and that information about these plots cannot be disclosed for various reasons. One possible source of this ominous feeling is the “Threat Matrix,” a spreadsheet in which thousands of leads are paraded daily before top government decision makers. As Graff (2011, pp. 19, 489, 345) vividly describes the process, it comes off as “a catalogue of horrors,” as the “daily looming prognoses of Armageddon.” According to former CIA Director George Tenet (2007, p. 232), “You could drive yourself crazy believing all or even half of what was in it.” This perspective is stressed as well by another insider who notes that the constant stream of scary information, combined with a “want of actionable intelligence,” led not to the conclusion that there was nothing to find, but rather to “an aggressive, panicked attitude that assumed the worst about threats” (Goldsmith 2007).

But given this mentality and given the record of the terrorist events that have actually occurred since 9/11, the claims of many averted but undisclosed terrorist attacks should at this point be taken with a grain of salt. Few, if any, of the disclosed terrorist plots remotely justify panic, and it is difficult to believe that it is only the big ones we haven’t heard about. Moreover, when terrorist plots have been blocked, it certainly appears that policing agencies generally have been

anything but tight-lipped about their accomplishment (Johnston and Shane 2009; Graff 2011, pp. 368; Aaronson 2013, pp. 202–6, 215–16). The *Washington Post's* Dana Priest says she frequently heard claims about averted but undisclosed plots from counterterrorism agencies and government officials. In response, she says she “asked them to share with us anything they could, plots that were foiled that we could put in the paper because we didn’t have many examples. We said give us things, just in generalities.” But “we didn’t receive anything back” (National Public Radio 2010).

Underestimating Terrorism because of Alternative Charges?

Terrorism arrests and indictments are made, of course, only when prosecutors think they have evidence to obtain a conviction. However, it could be that authorities have encountered aspirational terrorists, but lacking enough evidence to convict on terrorism charges, instead have levied lesser charges, such as immigration violations. One FBI estimate, in fact, is that only one terrorism case in four leads to terrorism charges, while simpler criminal charges are used with other cases (Graff 2011, pp. 420–21, 557; but see also Nakashima 2013).

A number of people assumed to be potential terrorists have thus been picked up and then convicted on minor charges. Some of these were deported and so have presumably vanished from the picture. Others, however, were given short sentences and then released. None in this latter group appear, upon release, to have ever done or plotted terrorism later: they do not come up in the 54 cases of terrorism since 2011 (Mueller 2014). This means either 1) that they were never potential terrorists in the first place, or 2) that all their terrorism leanings evaporated when they were picked up on minor charges. If the latter, they don’t seem to have been terribly dedicated to the cause.

What about Deterred Terrorists?

One can hypothesize that a number of potential terrorists pulled back from actually committing violence because they were intimidated by security measures. For example, insofar as military installations have been targeted in the United States, these have typically been recruiting offices within cities, not military bases, which are far more secure.

However, although security measures may have complicated terrorism planning in some cases, no dedicated would-be terrorist would have much difficulty finding other potential targets if the goal is to make a statement by killing people or destroying property. If security measures deter terrorism, they must primarily do so not because they are so effective, but rather because the would-be terrorists are not very dedicated in the first place and are rather easily dissuaded. Moreover, the notion that many terrorists are deterred needs to grapple with why were there so few plots in the months and years following the September 11 attacks, before enhanced security measures were effectively deployed. It may be that counterterrorism efforts are more likely to waylay impotent scheming than to prevent consummated violence.

What about the Smart Terrorists?

There is an argument that we only catch the incompetent terrorists, while the smart ones get away. But more than a decade after 9/11, one needs to explain why all these lurking would-be smart terrorists have not yet actually *done* something. It may be that smart people are dissuaded from committing terrorism not because of counterterrorism measures, but rather from the realization that no matter how deeply-felt their grievances and outrage, expressing them in random or semi-random civilian destruction is likely to be counterproductive to their cause (Abrahms 2011).

Conclusion

It is inevitably difficult to evaluate the appropriate level of counterterrorism spending, and even harder to evaluate the extent to which marginal increases in that spending are justified. But given the great expansion in resources devoted to counterterrorism spending as well as the opportunity costs of time and privacy, grappling with the question of how much counterterrorism spending is appropriate is not a question to be sidestepped.

Our approach supplies a framework for dealing with this question. Our calculations do suggest that for much counterterrorism spending to be justified, it would need to avert an implausibly high number of attacks of very substantial size every year. However, our analysis also suggests that FBI counterterrorism spending would be justified if, on its own, it prevents one attack of 9/11 magnitude every 60 years. Some might find that plausible enough to justify the FBI expenditures. Others might be inclined to consider 9/11 to be an aberration, stressing the fact that the human damage it inflicted was seven times higher than any other terrorist attack in history whether in war zones or not, while the property destruction it inflicted was even more exceptional.

Similarly, returning to what we have called “extended costs,” one might argue that if counterterrorism spending undercuts the political impetus for a costly protracted war, then such spending would be worthwhile. But although counterterrorism spending could in theory be a substitute for war, after 9/11 the two were complementary public policies as the United States did both.

Or one might argue that a heightened anxiety about terrorism, as opposed to other potential dangers, generates fear and engages the emotions much more than other hazards to human life, and therefore it justifies a relatively high level of spending. But that conclusion may be too broad: for example, the terrorist tragedy at Fort Hood in 2009 did not seem to cause widespread fear and anxiety, nor did it have much of an economic effect. It could also be maintained that officials in charge of public safety—the foundational reason for government—need to be roughly, if not necessarily completely, risk neutral (Sunstein 2006). Indeed, the Office for Management and Budget (1992) and most international regulators recommend a risk-neutral approach. However, homeland security decisions are often exceedingly risk averse: few, if any, government agencies, including

the Nuclear Regulatory Commission and the Environmental Protection Agency, exhibit anywhere near this level of risk aversion in their public decision making (for an expected utility analysis of United States homeland security spending, see Stewart, Ellingwood, and Mueller 2011). From this perspective, it is irresponsible for public officials and regulators to give in to political and emotional pressures and spend public and social resources on measures that save few lives when the same resources, used otherwise, might save many (Mueller and Stewart 2014).

The case for or against the increased levels of counterterrorism spending necessarily rests on such arguments. Another important reason for considering costs and benefits of counterterrorism spending is that it puts other types of security expenditures into contrast. For example, whatever one's conclusion about the benefit–cost ratio of the FBI's counterterrorism efforts, they are certainly superior to some other security measures. For example, the Transport Security Administration's Federal Air Marshal Service and its full body scanner technology together are nearly as costly as the entire FBI counterterrorism budget, but their risk reduction over the alternatives appears to be negligible (Mueller and Stewart 2011; Stewart and Mueller 2011, 2013a, 2013b). Moreover, the body scanner technology only deals with specific threats associated with hijacking and body-borne bombs on aircraft. In comparison, enhanced FBI expenditures would seem a preferable option: they deal with all terrorism threats, almost certainly do reduce the terrorism threat, and can be rapidly deployed or redeployed as threats emerge or evolve.

References

- Aaronson, Trevor.** 2013. *The Terror Factory: Inside the FBI's Manufactured War on Terrorism*. Brooklyn, NY: Ig Publishing.
- Abrahms, Max.** 2011. "Does Terrorism Really Work? Evolution in the Conventional Wisdom since 9/11." *Defence and Peace Economics* 22(6): 583–94.
- Bunn, Matthew, Anthony Weir, and John P. Holdren.** 2003. *Controlling Nuclear Warheads and Materials: A Report Card and Action Plan*. Washington, DC: Nuclear Threat Initiative and the Project on Managing the Atom, Harvard University.
- Bureau of Economic Analysis, US Department of Commerce.** 2013. "Economic Growth Widespread across Metropolitan Areas in 2012." News Release, September 17.
- Federal Bureau of Investigation, US Department of Justice.** 2013. *FY 2014: Authorization and Budget Request to Congress*. April. <http://www.justice.gov/jmd/2014justification/pdf/fbi-justification.pdf>.
- Goldsmith, Jack.** 2007. *The Terror Presidency: Law and Judgment Inside the Bush Administration*. New York: W. W. Norton & Co.
- Graff, Garrett M.** 2011. *The Threat Matrix: The FBI at War in the Age of Global Terror*. New York: Little, Brown, and Co.
- Johnston, David, and Scott Shane.** 2009. "Terror Case Is Called One of the Most Serious in Years." *New York Times*, September 24.

- LaTourrette, Tom, David R. Howell, David E. Mosher, and John MacDonald.** 2006. *Reducing Terrorism Risk at Shopping Centers: An Analysis of Potential Security Options*. Technical Report TR-41. Santa Monica, CA: RAND.
- Meade, Charles, and Roger C. Molander.** 2006. *Considering the Effects of a Catastrophic Terrorist Attack*. Technical Report TR-391-CTRMP. Santa Monica, CA: RAND.
- Mueller, John.** 2010. *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al Qaeda*. New York: Oxford University Press.
- Mueller, John, ed.** 2014. *Terrorism since 9/11: The American Cases*. Columbus, OH: Mershon Center, Ohio State University. <http://politicalscience.osu.edu/faculty/jmueller//since.html>.
- Mueller, John, and Mark G. Stewart.** 2011. *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security*. New York: Oxford University Press.
- Mueller, John, and Mark G. Stewart.** 2012. "The Terrorism Delusion: America's Overwrought Response to September 11." *International Security* 37(1): 81–110.
- Mueller, John, and Mark G. Stewart.** 2014. "Terrorism and Counterterrorism in the US: The Question of Responsible Policy-Making." *International Journal of Human Rights* 18(2): 228–40.
- Nakashima, Ellen.** 2013. "Audit: Justice Department Office Overstated Terrorism Conviction Statistics." *Washington Post*, September 17.
- National Public Radio.** 2010. "Intelligence Failures in 'Top Secret America.'" *Talk of the Nation*, transcript, July 19.
- National Research Council of the National Academies.** 2010. *Review of the Department of Homeland Security's Approach to Risk Analysis*. Washington, DC: National Academies Press.
- Office of Management and Budget.** 1992. *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs (Revised)*, October 29. Circular No. A-94. Washington, DC.
- Robinson, Lisa A., James K. Hammitt, Joseph E. Aldy, Alan Krupnick, and Jennifer Baxter.** 2010. "Valuing the Risk of Death from Terrorist Attacks." *Journal of Homeland Security and Emergency Management* 7(1): Article 14.
- Stewart, Mark G., Bruce R. Ellingwood, and John Mueller.** 2011. "Homeland Security: A Case Study in Risk Aversion for Public Decision-Making." *International Journal of Risk Assessment and Management* 15(5/6): 367–86.
- Stewart, Mark G., and John Mueller.** 2011. "Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening." *Journal of Homeland Security and Emergency Management* 8(1): Article 30.
- Stewart, Mark G., and John Mueller.** 2013a. "Terrorism Risks and Cost-Benefit Analysis of Aviation Security." *Risk Analysis* 33(5): 893–908.
- Stewart, Mark G., and John Mueller.** 2013b. "Aviation Security, Risk Assessment, and Risk Aversion for Public Decisionmaking." *Journal of Policy Analysis and Management* 32(3): 615–33.
- Stiglitz, Joseph E., and Linda J. Biles.** 2008. *The Three Trillion Dollar War*. New York: Norton.
- Sunstein, Cass R.** 2006. "Misfearing: A Reply." University of Chicago, John M. Olin Program in Law and Economics Working Paper No. 274.
- Tenet, George.** 2007. *At the Center of the Storm: My Years at the CIA*. With Bill Harlow. New York: HarperCollins.

This article has been cited by:

1. Avishai Melamed, Adi Rao, Sarah Kreps, Erika Palmer. 2024. Popular impact: Public opinion and planetary defense planning. *Acta Astronautica* **214**, 505-525. [[Crossref](#)]
2. Lee Jarvis. 2023. Critical terrorism studies and numbers: engagements, openings, and future research. *Critical Studies on Terrorism* **16**:4, 720-743. [[Crossref](#)]
3. Rafat Mahmood, Michael Jetter. 2023. Gone with the wind: The consequences of US drone strikes in Pakistan. *The Economic Journal* **133**:650, 787-811. [[Crossref](#)]
4. Mukesh Eswaran, Hugh M. Neary. 2022. Decentralised Terrorism, Religion, and Social Identity. *Journal of Economics, Management and Religion* **03**:01. . [[Crossref](#)]
5. Tamara Stotz, Angela Bearth, Signe Maria Ghelfi, Michael Siegrist. 2022. The perceived costs and benefits that drive the acceptability of risk-based security screenings at airports. *Journal of Air Transport Management* **100**, 102183. [[Crossref](#)]
6. Lee Jarvis. 2022. Critical terrorism studies and the far-right: beyond problems and solutions?. *Critical Studies on Terrorism* **15**:1, 13-37. [[Crossref](#)]
7. Mark G. Stewart, John Mueller. Aviation Resilience to Terrorist Hijackings 69-91. [[Crossref](#)]
8. Shuai Chen. 2022. Rally Post-Terrorism. *SSRN Electronic Journal* **93**. . [[Crossref](#)]
9. Mark G. Stewart. 2021. Terrorism Risks and Economic Assessment of Infrastructure Protection against Progressive Collapse. *Journal of Structural Engineering* **147**:10. . [[Crossref](#)]
10. Andrew E Clark, Orla Doyle, Elena Stancanelli. 2020. The Impact of Terrorism on Individual Well-Being: Evidence from the Boston Marathon Bombing. *The Economic Journal* **130**:631, 2065-2104. [[Crossref](#)]
11. Sheraz Ahmad Choudhary, Muhammad Azhar Khan, Abdullah Zafar Sheikh, Mohd Khata Jabor, Mohd Safarin bin Nordin, Abdelmohsen A. Nassani, Saad M. Alotaibi, Muhammad Moinuddin Qazi Abro, Xuan Vinh Vo, Khalid Zaman. 2020. Role of information and communication technologies on the war against terrorism and on the development of tourism: Evidence from a panel of 28 countries. *Technology in Society* **62**, 101296. [[Crossref](#)]
12. Warren S. Eller, Adam S. Wandt. 2020. Contemporary Policy Challenges in Protecting the Homeland. *Policy Studies Journal* **48**:S1. . [[Crossref](#)]
13. Mark G. Stewart, John Mueller. 2020. Terrorism risks, chasing ghosts and infrastructure resilience. *Sustainable and Resilient Infrastructure* **5**:1-2, 78-89. [[Crossref](#)]
14. Shuai Chen. 2020. Rally Post-Terrorism. *SSRN Electronic Journal* **93**. . [[Crossref](#)]
15. Eugen Dimant, Tim Krieger, Daniel Meierrieks. 2020. Paying Them to Hate US: The Effect of U.S. Military Aid on Anti-American Terrorism, 1968-2014. *SSRN Electronic Journal* **26**. . [[Crossref](#)]
16. Pritha Dev, Konrad Grabiszewski. 2019. More Is Not Always Better: The Case of Counterterrorism Security. *Journal of Conflict Resolution* **63**:8, 1923-1938. [[Crossref](#)]
17. Ishmael Tingbani, Godwin Okafor, Venancio Tauringana, Alaa Mansour Zalata. 2019. Terrorism and country-level global business failure. *Journal of Business Research* **98**, 430-440. [[Crossref](#)]
18. Michael Jetter, David Stadelmann. 2019. Terror per Capita. *Southern Economic Journal* **96**. . [[Crossref](#)]
19. Mark G. Stewart, John Mueller. 2018. Risk and economic assessment of U.S. aviation security for passenger-borne bomb attacks. *Journal of Transportation Security* **11**:3-4, 117-136. [[Crossref](#)]
20. Abel Brodeur. 2018. The Effect of Terrorism on Employment and Consumer Sentiment: Evidence from Successful and Failed Terror Attacks. *American Economic Journal: Applied Economics* **10**:4, 246-282. [[Abstract](#)] [[View PDF article](#)] [[PDF with links](#)]

21. Mark G. Stewart, John Mueller. Reducing Costs Without Reducing Security: Comparing the Value of Individual Layers 99-133. [[Crossref](#)]
22. Matthew J. Grant, Mark G. Stewart. 2017. Modelling improvised explosive device attacks in the West – Assessing the hazard. *Reliability Engineering & System Safety* **165**, 345-354. [[Crossref](#)]
23. Mark G. Stewart, John Mueller. 2017. Risk and economic assessment of expedited passenger screening and TSA PreCheck. *Journal of Transportation Security* **10**:1-2, 1-22. [[Crossref](#)]
24. Matthew J. Grant, Mark G. Stewart. 2017. Benefit of Distributed Security Queuing for Reducing Risks Associated With Improvised Explosive Device Attacks in Airport Terminals. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering* **3**:2. . [[Crossref](#)]
25. Mark G. Stewart. 2017. Risk of Progressive Collapse of Buildings from Terrorist Attacks: Are the Benefits of Protection Worth the Cost?. *Journal of Performance of Constructed Facilities* **31**:2. . [[Crossref](#)]
26. Mark G. Stewart. Risk and Decision-Making for Extreme Events: Climate Change and Terrorism 87-103. [[Crossref](#)]
27. Matthew Grant, Mark G. Stewart. 2015. Probabilistic Risk Assessment for Improvised Explosive Device Attacks That Cause Significant Building Damage. *Journal of Performance of Constructed Facilities* **29**:5. . [[Crossref](#)]
28. Javier Gardeazabal, Todd Sandler. 2015. INTERPOL's Surveillance Network in Curbing Transnational Terrorism. *Journal of Policy Analysis and Management* **34**:4, 761-780. [[Crossref](#)]
29. Willem de Lint, Wondwossen Kassa. 2015. Evaluating U.S. Counterterrorism Policy: Failure, Fraud, or Fruitful Spectacle?. *Critical Criminology* **23**:3, 349-369. [[Crossref](#)]