2011-09

How Proverbs Damage Homeland Security

Bellavita, Christopher

Monterey, California. Naval Postgraduate School

Homeland Security Affairs (September 2011), v.7 no.2
http://hdl.handle.net/10945/24990

How Proverbs Damage Homeland Security

Christopher Bellavita

Proverbs express significant truths about a cultural narrative.[1] They communicate values, beliefs and knowledge. John Dewey wrote: "The consequences of a belief upon other beliefs and upon behavior may be so important ... that [people] are forced to consider the grounds or reasons of their belief and its logical consequences."[2] Dewey described the "consideration" as reflective thought, or what a century later is called critical thinking.

Proverbs helped construct homeland security's narrative during its first decade. The ideas they transmitted reduced ambiguity and gave strategic direction to the new national enterprise.

But proverbs can inhibit as much as enhance. Sometimes the "truth" they embody escapes scrutiny, inhibiting efforts to allow a narrative to evolve. Herbert A. Simon wrote: "If it is a matter of rationalizing behavior that has already taken place or justifying action that has already been decided upon, proverbs are ideal.... [They] are a great help in persuasion, political debate, and all forms of rhetoric."[3]

Homeland security's first decade was characterized by "ready, fire, aim." A great deal of work had to be done in a short period of time. Much was accomplished during that decade, and it cost a lot of money. By one estimate more than one trillion dollars was spent on homeland-related programs during the decade.[4] No one knows how much of that money went to ineffective activities because the homeland security enterprise spent more effort firing than aiming.

Homeland security's second decade can productively focus on "aiming." Academics and strategists have an opportunity to critically examine the basic assumptions underpinning the homeland security narrative, and identify evidence that supports or refutes foundational ideas used to guide strategic direction. The purpose of this essay is to illustrate such an examination.

Here are one dozen proverbs that partially outline the homeland security narrative:[5]

1. Intelligence analysts need to connect the dots.
2. They [the "enemy"] hate us for our freedoms.
3. We fight them over there so we don't have to fight them here.
4. Risk is a function of threat, vulnerability, and consequence.
5. All disasters are local.
6. All hazards means *all* hazards.
7. To be prepared get a kit, make a plan, and be informed.
8. If you see something, say something.
9. People are likely to panic in a disaster.
10. Those who would give up essential liberty to purchase a little temporary security deserve neither liberty nor security.
11. Terrorists only have to be lucky once; we have to be lucky all the time.
12. Eight-five percent of US critical infrastructure is owned/controlled/in-the-hands-of/operated by [the verbs change] the private sector.

I think the proverbs are wrong or misleading in important respects. As a consequence, they distort the homeland security narrative and inhibit the search for more effective ideas to protect the nation. My overall claim is based on a mix of anecdote, suggestive evidence, and hunch. I discuss one proverb in depth (*Eight-five percent of US critical infrastructure is owned by the private sector*) and assert the others can also benefit from critical analysis.

The 85 percent figure is probably America's best-known homeland security statistic. The claim appears in the 9/11 Commission hearings, the *9/11 Commission Report*, the 2002 and the 2007 national homeland security strategies, and stacks of related documents.[6] It is parroted by Congress, the DHS, think tanks, academics, trade associations, and other homeland

security residents.[7] Its presence is not restricted to our borders. The number appears also in Canadian and Czech Republic reports about who owns their critical infrastructure.[8]

I will describe my efforts over the past decade to understand what the 85 percent claim means and offer four reasons why uncritically accepting the proverb as truth harms homeland security. I close by suggesting why the other proverbs may also be misleading.

WHAT DOES THE NUMBER MEAN?

What could the 85 percent number mean, even in principle? Is there a difference that matters between "ownership," "control," "in-the-hands-of," or "operated?"

I can come to terms with the inability to know with certainty what homeland security is. But what explains the difficulty agreeing who or what controls critical infrastructure?

Maybe the quandary rests in how the claim is structured. Sometimes the number refers simply to all "infrastructure."[9] Other times it's about "critical" infrastructure.[10]

But putative distinctions may no longer matter. The initial difference between critical infrastructure and plain vanilla infrastructure seems to have quietly vanished.

Critical infrastructure used to mean what the USA PATRIOT Act directed it to mean:

> Systems and assets, whether physical or virtual, **so vital to the United States** that the incapacity or destruction of such systems and assets would have a debilitating impact on security, **national** economic security, **national** public health or safety, or any combination of those matters.[11] [My emphasis.]

In 2009, a different definition of critical infrastructure appeared in the National Infrastructure Protection Plan:

> Systems and assets, whether physical or virtual, **so vital** that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, **across any Federal, State, regional, territorial, or local jurisdiction**.[12] (My emphasis again.)

The "flea markets, petting zoos, popcorn factories, hot dog stands or other such facilities" DHS was (unreasonably) criticized for including in a critical assets database a few years ago may turn out to be someone's critical infrastructure after all.[13]

Compounding the semantic problem, how could one even estimate, let alone calculate with any precision, ownership or control?[14] Does one identify every individual provider of goods and services that could be included in the (18, 19, or more) sectors,[15] discover who owns (in some legal sense) each business, and then determine percentages? Does one classify companies and organizations into the sectors first, then figure out who owns the sectors and calculate from that premise? Is ownership equivalent to control? Does ownership or control imply government has little to no say in security practices?

A July 2011 Congressional Research Service Report observed,

> Sharing information with the federal government about vulnerability assessments, risk assessments, and the taking of additional protective actions is meant to be voluntary. However, the degree to which some of the activities are mandated varies across sectors. In some cases, sectors are quite regulated.[16]

The answer to whether the distinction between public or private control has substantive meaning is "yes, no, and it depends."

But what about the 85 percent proverb? How does it harm homeland security?

WHEN PEDANTRY MATTERS

The word "pedantry" was invented to refer to an excessive concern with petty details.[17] One might say anguishing over 85 percent is pedantry.

One author who writes about critical infrastructure noted,

> Whether this figure is 100 percent accurate or based on any in-depth analysis is debatable but, regardless, little or no infrastructure would function (critical or otherwise) without the efforts of private sector owners and operators.[18]

A senior DHS official addressed my distress more directly a few years ago: "It

doesn't matter whether the 85 percent is right or not," he said. "We're still going to do the same thing."

I believe it does matter. And by "it" I mean the persistence of an idea that impedes considering alternative ideas about how to protect critical infrastructure.

Here are four reasons why the proverb's persistence damages homeland security. A discussion of each reason follows.

1. It gives the impression we know more than we do when it comes to critical infrastructure.
2. It creates a false image about the power relationships between the public and private sectors.
3. It distorts normative understanding about roles and responsibilities.
4. It constrains discussions about policy options.

THE IMPRESSION OF COMPETENCE

The philosopher Harry Frankfurt writes about the distinction between those who tell the truth or who lie, and those who bullshit. Truth tellers and liars cohere around the truth, either to communicate it or to hide it. One who uses bullshit does not care about the truth or falsity of a claim, but instead cares about the impression the claim makes. Bullshit substitutes sincerity for accuracy.[19]

"Maybe we don't know the truth about critical infrastructure," the reasonable homeland security professional might argue, "but the claim is well-meaning; work with me here so we can do good."

The sincerity underpinning the 85 percent myth gives an impression that when it comes to critical infrastructure we fundamentally know what we are talking about. More specifically, quantifying ownership and control signals someone knows what infrastructure is actually critical, and professionals can thus manage what is vital to the nation's security and well-being.

The number's misguided precision veils what we do know: there is no "one definite prioritized list of critical assets…" and "it would not be possible or useful to develop one."[20]

PRIVATE POWER, PUBLIC POWER

The 85 percent number conveys an inference about the power relationships between the public and private sector: since the important parts of the nation are owned by the private sector, government ought to "ask" the private sector to help out with this messy security business. The private sector can, of course, decline.

There is another – less discussed – side to the power assessment. The 85 percent benediction does not automatically advantage the private sector. Some infrastructure officials, nominally in the private sector, say the 85 percent figure justifies preventing the private sector from receiving information, grants and other public funds needed to upgrade and secure their facilities.

> The dilemma… has been in encountering an obdurate, logic-proof insistence by cops, fire fighters, emergency managers, fusion center staff, and DHS minions to define my employer and all critical infrastructure stewards as private sector entities… [and thus] unworthy of [receiving] sensitive information… and inherently suspect of being profit driven….[21]

I have not found data describing how well the private sector embraces its sometimes-reluctant partnership in the homeland security enterprise.[22] I have heard anecdotes about industries that take seriously the part they play in ensuring the nation's security.[23] I also hear stories about the predictable cast of characters showing up at regularly scheduled gatherings arranged to praise or encourage public-private infrastructure partnerships.

I have not seen the comprehensive metrics across critical sectors a chief financial officer or board of directors would demand about the impact of those partnerships. But the same can be said for evidence about the public sector's contribution to preparedness and resilience.[24] Maybe when it comes to infrastructure neither sector has as much power as the other believes.

OWNERSHIP IS NOT RELEVANT

It may be rhetorically convenient to separate public and private sector responsibilities. But assuming what has yet to be demonstrated interferes with determining who has to do what to strengthen protection.

One of my colleagues views the "who owns what" argument this way:[25]

> The argument is bogus: the big stuff, like water, power, energy, transportation is so regulated and controlled by the feds, that the fact that it is owned by someone isn't a factor. If the feds decided to harden power plants, for example, Congress can do what it wants. Isn't this the case already with nukes and the Federal Energy Regulatory Commission? Same thing with transportation, energy, etc.

Another colleague expressed his concern about responsibilities:[26]

> The basic foundation of our society – [the] infrastructure that is essential for public safety and well-being – is owned and controlled by state and local government.[27] .... The underlying premise behind having much of this [infrastructure] under state and local control is they are monopolies or they are so critical that from a societal aspect you cannot have a company that runs any of this infrastructure go [into] Chapter 7.

Critical infrastructure is too critical to be left to the private sector to protect, he argued. Policymakers need to acknowledge the partnership between the invisible hand of free enterprise and another hand:

> There is a second "hidden" [and] "unseen hand" to much of this infrastructure. This is the state regulatory agencies. The regulatory construct is what holds this all together and without which the sectors could not function. Food and agriculture, water systems, health systems cannot function without the regulatory agencies (mostly state government) functioning.

Trying to determine who owns what is less productive than identifying contributions different sectors make to disparate types of security and resiliency:

> [Our] state governments should actually be our primary infrastructure partner and primary partner in [societal] security and resiliency. The private sector who employs most of the work force and generates a huge percentage of GDP should be our primary partner in economic security and economic resiliency. Both are our partners in disaster resiliency. Most of our [critical infrastructure] does not produce GNP it enables GNP but does not produce anything. Thus from an economic standpoint we should focus attention on the GNP producers. This is why separation between enablers and producers is counterproductive.... We have also made a strategic mistake in [putting] all infrastructure into the "private sector" domain regarding business models. State and local government business models and the business model of a company on the stock exchange are completely different.

HIDING THE NETWORKS

Thinking about ownership and control encourages strategists and policymakers to consider critical infrastructure primarily as a collection of "eaches" – individual farms, water treatment plants, monuments, dams, power plants, manufacturers – to be protected. But "most critical infrastructure spans multiple states." Gas and oil pipelines, electric power grids, telecommunications networks, Internet and computer networks, water supplies, food, chemical and industrial networks "all cross state boundaries."[28]

The "eaches" framework that flows from the 85 percent mantra obscures policy options premised on a network view of infrastructure. Considering infrastructure as networks draws attention to nodes, links, interdependencies, scale free structures, power laws, small worlds, self-organized criticality, sand piles, and related concepts that might inspire innovative approaches to protecting infrastructure.[29]

WHAT ELSE?

Debate about the 85 percent number is operationally trivial. But questioning whether it is valid can remind those of us in the homeland security enterprise to critically examine what we accept as true. If we got the 85 percent wrong, yet it persists as truth, what else have we missed?

Revisiting the proverbs introduced at the start of the essay suggests possible answers to that question.

1. Intelligence analysts may be expected to connect the dots, but the expectation ignores the complexity of the intelligence task. "[Pleading] for more dots is to mistake the nature of the problem posed by … terrorism, and … even recognizing the significance of the information is a task that exceeds the capacity of a single organization…." [30]
2. One may believe the enemy hates us for our freedoms, but one must also listen to the argument that "blaming our freedoms for Muslim terror is absurd and dangerous." [31]
3. We fight them over there so we don't have to fight them here, but the growing concern about domestic radicalization suggests this proverb needs to be retired. [32]
4. Risk might be a function of threat, vulnerability, and consequence, but in homeland security the nature of, and data sources for, that function remain illusive. [33]
5. All disasters may once have been local, but in homeland security's second decade, one may need to acknowledge "disasters have far-reaching consequences throughout regions, states, the nation and even the globe." [34]
6. All hazards does not really mean *all* hazards. As one of the nation's respected emergency management scholars explained, "*All-hazards* does not literally mean being prepared for any and all hazards that might manifest themselves in a particular community, state, or nation." It does mean developing a general plan that "can provide the basis for **responding** to unexpected events." [35] [My emphasis.]
7. Getting a kit, making a plan and staying informed may be one theory about preparedness, but the advice does not appear to resonate with the American people. One state emergency management director suggested,

   > We need to reframe expectations. A disaster kit, prepackaged and stored away only to be used in a disaster is not practical for many Americans. It is costly and takes time, attention, and desire to maintain…. We must educate the public about the risks they actually face, have an honest discussion with them about what they expect government to do, what they can do and, more to the point, what they must do. Then we need to ask how we can help them be better prepared. But not through another revised seventy-two-hour preparedness campaign with the same messages we are promoting today. [36]

8. If you see something, say something, but what gets said, and with what effect? The Metropolitan Transit Authority created the trademarked slogan shortly after the 9/11/01 attacks. It has since been leased to the Department of Homeland Security. Is this proverb an effective way to engage citizens in homeland security, is it eyewash, or is it pernicious? [37] One security expert cautioned, "if you ask amateurs to act as front-line security personnel, you shouldn't be surprised when you get amateur security. People don't need to be reminded to call the police; the slogan is nothing more than an invitation to report people who are different." [38]
9. The idea that people are likely to panic in a disaster persists in the face of convincing evidence to the contrary. As one example, a study of over 500 disaster events concluded: "panic was of very little practical or operational importance." [39]
10. People who agree with Benjamin Franklin's 1775 homily that "Those who would give up essential liberty to purchase a little temporary security deserve neither liberty nor security," may ignore the suggestion raised by Philip Bobbitt that in *The Wars for the Twenty-First Century* "it is possible to increase the powers of government and, at the same time, increase the rights of the people." [40]
11. The belief "Terrorists only have to be lucky once; we have to be lucky all the

time" originated in a terrorist message issued after the 1984 Brighton bombing.[41] US policymakers adapted the language and turned it into a strategic proverb.[42] One American WMD expert countered that claim by noting terrorists planning a complex operation have to worry about many pieces coming together. "They have to be right all the time," he said. "We only have to be right once to stop them."[43]

WHAT IS YOUR CLAIM AND WHY SHOULD ANYONE BELIEVE IT?

The proverbs discussed in this essay may turn out eventually to be approximately right or substantially wrong. As Herbert Simon wrote about a different set of proverbs:

> It is not that the propositions expressed by the proverbs are insufficient; it is rather that they prove too much.... For almost every principle one can find an equally plausible and contradictory principle...and there is nothing...to indicate which is the proper one to apply.[44]

A 2011 study described homeland security as an "anemic policy regime," whose purposes are "poorly understood and not widely shared among different elements of the federal government or at subnational levels." It is characterized by "the weakness of the integrative ideas of 'homeland security' and 'all hazards' preparedness, the lack of a strong constituency for the regime, and the institutional misalignment among relevant subsystems."[45]

That critique does not flatter the organizations and people who shaped the homeland security enterprise. But the study's conclusions are based on evidence not slogans. One can agree or disagree with the authors' assumptions, analysis, and conclusions, but one does not have to guess how those conclusions were derived.

Homeland security's second decade ought to evolve toward a narrative foundation constructed by something more substantial than proof by repeated assertion. One should ask for evidence.

ABOUT THE AUTHOR

Christopher Bellavita *teaches at the Naval Postgraduate School in Monterey, California, where he serves as the director of academic programs for the Center for Homeland Defense and Security. Dr. Bellavita is the executive editor of* Homeland Security Affairs*, and a contributing editor to the* Homeland Security Watch *blog.*

---

1 I'd like to thank three reviewers who provided comments that helped improve this essay. I am using proverb in the sense described in the Oxford English Dictionary: "A ... concise sentence ... stating a general truth or piece of advice...." I think arguments could be made that what I am describing could also be called myth ("a widespread but untrue or erroneous ... belief; a widely held misconception...") or meme ("a cultural element ... whose transmission and consequent persistence in a population ... is considered as analogous to the inheritance of a gene").

2 John Dewey, *How We Think* (Boston: D.C. Heath & Co, 1910), 5.

3 Herbert A. Simon, "The Proverbs of Administration," *Public Administration Review* 6, Winter (1946), 53.

4 John Mueller and Mark G. Stewart. "Balancing the Risks, Benefits, and Costs of Homeland Security," *Homeland Security Affairs* 7, Article 16 (August 2011) http://www.hsaj.org/?article=7.1.

5 Lauren Wollman noted in a personal correspondence that "however empty or inaccurate [the proverbs may be], ... they serve the critical function in the emergence of the idea [of homeland security]: they facilitate the construction of a narrative and the transmission of specialized knowledge and lexicon to and from lay-culture.... In some ways... is it not more interesting to know why those particular images and proverbs [were adopted] to begin with? What story they tell, what truths they solidify in our imagination, what truths and facts they create?" She also added "need to know vs. need to share," and "stovepipes are bad, collaboration is good" as candidate proverbs.

6 See http://govinfo.library.unt.edu/911/archive/hearing5/9-11Commission_Hearing_2003-11-19.htm; National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 1st ed. (New York: Norton, 2004), 398; United States, *National Strategy for Homeland Security* (Washington, D.C.: Office of Homeland Security, 2002) 33. Homeland Security Council, *National Strategy for Homeland Security* (October 2007), 4.

7 For examples see Christopher Bellavita, "85% of what you know about homeland security is probably wrong," *Homeland Security Watch* (blog), March 16, 2009, http://www.hlswatch.com/2009/03/16/85-percent-is-wrong/, especially the insightful comments. The most recent instance I've seen of the number in print is testimony at the House Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, March 16, 2011 by James A. Lewis, "Examining the Cyber Threat to Critical Infrastructure and the American Economy," 4. On August 15, 2011, while this paper was being prepared, I heard the number used during a conference of homeland security professionals: "As every one knows," the speaker said, "85 percent of our critical infrastructure is directed by the private sector."

8 For Canada, see http://www.homelandsecuritynewswire.com/unprepared-canada-lacks-plan-protect-critical-infrastructure. For the Czech Republic, see http://bit.ly/ofI5wv.pdf.

9 For example, see Paul C. Robinson, Joan B Woodard, and Samuel G. Varnado, "Critical Infrastructure: Interlinked and Vulnerable," *Issues in Science and Technology*, Fall (1998), www.issues.org/15.1/Robins.htm.2. This article is one of the earliest written examples I've found of the 85 percent number.

10 For example, see "What is CIP?" http://cip.gmu.edu/component/k2/item/118-what-is-cip?

11 As noted in Department of Homeland Security, *Interim National Infrastructure Protection Plan* (February 2005), 3: "USA PATRIOT Act of 2001, 42 U.S.C. § 5195c(e), defining critical infrastructure. This definition is incorporated by reference into the Homeland Security Act of 2002, see 6 U.S.C. § 101."

12 Department of Homeland Security, *National Infrastructure Protection Plan* (2009), 109.

13 Robert Stephan, "Database is Just the 1st Step," *USA Today,* July 21, 2006, 8A.

14 Charlie Jasonberg pointed out (http://www.hlswatch.com/2009/03/16/85-percent-is-wrong/#comment-134580): "One of the GMU CIP reports investigated the 85% claim for the water sector. It used EPA and other data, and learned that 61% of the water sector was owned by the private sector, with 28% owned by local governments. So, the [percent] will vary from industry-to-industry." http://cip.gmu.edu/archive/cip_report_6.4.pdf.

15 John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation* (Congressional Research Service, July 11, 2011), 17.

16 Ibid., 31

17 Philological Society (Great Britain), *The Oxford English Dictionary; Being a Corrected Re-Issue with an Introduction, Supplement, and Bibliography of A New English Dictionary on Historical Principles* VII (Oxford: At the Clarendon Press, 1933), 606.

18 Timothy P. Clancy, "CI/KR Public-Private Partnerships — Sharing Responsibility, Managing Risk," *The CIP Report* (July 2008), 17.

19 Harry G Frankfurt, *On Bullshit* (Princeton, NJ: Princeton University Press, 2005), 53-56, 65.

20 Moteff, *Critical Infrastructures,* 26. DHS does claim it knows the highest priority sites.

21 Nick Catrantzos quoted in Christopher Bellavita, "85% More From The Private Sector About Critical Infrastructure," *Homeland Security Watch* (blog), March 30, 2010, http://www.hlswatch.com/2010/03/30/85-more-from-the-private-sector-about-critical-infrastructure/.

22 Moteff, *Critical Infrastructures,* 16-31, reviews many of the difficulties encountered trying to create and sustain partnerships.

23 I was told in August 2011 that data do exist demonstrating the information technology (IT) community has "vigorously embraced its security relationship and responsibility with government." Once I find that data I will update this note.

24 See for example Christopher Bellavita, "Homeland Security's War On Subjectivity," *Homeland Security Watch* (blog), October 29, 2009, http://www.hlswatch.com/2009/10/29/homeland-securitys-war-on-subjectivity/.

25 T. G. Lewis, personal correspondence.

26 The three quotations are from personal correspondence with an executive who works with critical infrastructure for a federal agency.

27 Examples include landfills, water systems, reservoirs, wastewater systems, emergency services, roads, bridges, tunnels, airports, ports, parts of the electrical system, mass transit (rail and bus), dams, universities, prison systems, courts – legal system, county administration buildings, state office buildings, state laboratories, and state hospitals.

28 T. G Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, N.J: Wiley-Interscience, 2006), 47.

29 See, for examples, Ted G. Lewis, *Bak's Sand Pile* (Monterey: Agile Press, 2011); and Lewis, *Critical Infrastructure Protection in Homeland Security*.

30 Christopher Bellavita, "Nidal Hasan and the problem of connecting the dots," *Homeland Security Watch* (blog), November 12, 2009, http://www.hlswatch.com/2009/11/12/nidal-hasan-and-the-problem-of-connecting-the-dots/ citing Max Boisot.

31 Jonah Goldberg, "Free Speech and Burning Korans," *Townhall*, April 13, 2011, http://townhall.com/columnists/jonahgoldberg/2011/04/13/free_speech_and_burning_korans/page/2, quoting a 2007 statement by Dinesh D'Souza

32 Bob Johnson, "'Fight them there, so we don't have to fight them here' key lie in New Big Fib," *Daily Kos*, September 2, 2006, http://www.dailykos.com/story/2006/09/02/242333/-Fight-them-there,-so-we-dont-have-to-fight-them-here-key-lie-in-New-Big-Fib%C2%A9; Ron Paul, "'Fight them over there vs. over here' a false choice," *The Washington Times*, July 1, 2009, http://www.washingtontimes.com/news/2009/jul/01/fight-them-over-there-vs-over-here-presents-a-fals/; Jonah Czerwinski, "Fight'em Over There," *Homeland Security Watch* (blog), July 1, 2007, http://www.hlswatch.com/2007/07/06/fightem-over-there/; "New Reports on Terrorist Plots and Domestic Radicalization since 9/11," https://hsdl.org/hslog/?q=node/5534.

33 For one example of the variety of risk definitions, see http://www.sarma-wiki.org/index.php?title=Risk#_note-0. See also Unknown, "Incorporating Assessments of Terrorism Risk in Homeland Security Resource Allocation Decision Making: Closing the Gap Between Current and Needed Capabilities" (presented at the Risk Informed Decision Making for HLS Resource, Arlington, Virginia, 2009), 3: "The risk construct presented above [R = T x V x C] is logical, intuitively appealing, and consistent with conceptualizations of risk used in other domains. However, uncertainty inherent in deriving estimates for its components in the case of terrorism risk continues to compromise its usefulness in DHS resource allocation decision making. As a result, terrorism risk assessments have not played the prominent role they were expected to play in DHS resource allocation decision making. More robust and defensible methods for generating required inputs for this terrorism risk construct are required if it is to become an important factor in homeland security resource allocation decision making." For an insightful interpretation of the homeland security approach to risk, see Bob Ross, "The Multiple Levels of Risk Management," *Homeland Security Watch* (blog), April 2, 2009, http://www.hlswatch.com/2009/04/02/the-multiple-levels-of-risk-management/.

34 Jim Mullen, "Not all disasters are local," Washington Military Division; Emergency Management Department, March 23, 2011, http://blogemd.blogspot.com/2011/03/not-all-disasters-are-local.html. For another example, see Ashton B. Carter, Michael M. May, and William J. Perry, "The Day After: Action Following a Nuclear Blast in a U.S. City," *The Washington Quarterly* (Autumn 2007): 22-23.

35 "*All-hazards* does not literally mean being prepared for any and all hazards that might manifest themselves in a particular community, state, or nation. What it does mean is that there are things that commonly occur in many kinds of disasters, such as the need for emergency warning or mass evacuation, that can be addressed in a general plan and that that plan can provide the basis for responding to unexpected events." William Waugh, "Terrorism and the All-Hazards Model," 2004, http://training.fema.gov/EMIWeb/downloads/Waugh%20-%20Terrorism%20and%20Planning.doc.

36 Christopher Bellavita, "From kits to sustainment — reframing preparedness expectations and guidance," *Homeland Security Watch* (blog), March 8, 2011, http://www.hlswatch.com/2011/03/08/from-kits-to-sustainment-%E2%80%94-reframing-preparedness-expectations-and-guidance/, quoting Nancy Dragani.

37 William Neuman, "In Response to M.T.A.'s 'Say Something' Ads, a Glimpse of Modern Fears," *New York Times*, January 7, 2008, http://www.nytimes.com/2008/01/07/nyregion/07see.html. John Solomon, "New Study Indicates Difficulty In Evaluating Effectiveness Of 'See Something, Say Something'-Like Citizen Tips Campaigns," *In Case of Emergency, Read Blog*, September 17, 2010, http://incaseofemergencyblog.com/2010/09/17/new-study-indicates-difficulty-in-evaluating-effectiveness-of-see-something-say-something-like-citizen-tips-campaigns/.

38 Bruce Schneier, "If You See Something, Say Something," *Schneir on Security* (blog), May 12, 2010, http://www.schneier.com/blog/archives/2010/05/if_you_see_some.html.

39 Cited in Erik Auf der Heide, "Common Misconceptions about Disasters: Panic, the 'Disaster Syndrome,' and Looting," in *The First 72 Hours: A Community Approach to Disaster Preparedness* (Lincoln, Nebraska: iUniverse Publishing., 2004), 343.

40 Philip Bobbitt, *Terror and Consent: The Wars for the Twenty-First Century* (Knopf, 2008): 285-288.

41 'Today we were unlucky," [The Irish Republican Army communiqué] said, "but remember, we only have to be lucky once. You have to be lucky always. Give Ireland peace, and there will be no war.'" Jo Thomas, "This Time, the IRA Comes Close to Thatcher," *New York Times*, October 14, 1984, http://www.nytimes.com/1984/10/14/weekinreview/this-time-the-ira-comes-close-to thatcher.html?scp=2&sq=%93Terrorists+only+have+to+be+lucky+once%3B+we+have+to+be+lucky+all+the+time%94+&st=nyt.

42 Sean O'Driscoll, "U.S. Pols Quote IRA Statement," *Irish Voice*, n.d., http://www.irishabroad.com/news/irishinamerica/news/USPolsQuoteStatement.asp.

43 Al Mauroni, personal correspondence, reporting a statement originating from a federal law enforcement agency.

44 Simon, "The proverbs of Administration," 53.

45 Peter J. May, Ashley E. Jochim, and Joshua Sapotichne, "Constructing Homeland Security: An Anemic Policy Regime," *Policy Studies Journal* 39, no. 2 (2011): 302.