Homeland Security Affairs

Volume I, *Issue* 1 2005 *Article* 3

Summer 2005

What is Preventing Homeland Security?

Christopher Bellavita*

*Naval Postgraduate School, christopherbellavita@gmail.com

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
What is Preventing Homeland Security?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School ,Center for Homeland Defense and Security,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**13**	

What is Preventing Homeland Security?

Christopher Bellavita

Abstract

Almost four years have gone by since the United States formally joined the global war on terrorism. Yet something stops us from giving as much attention to preventing terrorism as we give to preparing to respond to the next attack. One reason is a homeland security system that is designed for response rather than prevention. Three fears hamper efforts to reconfigure that system: the fear of new behaviors; the fear of imagination; and the fear of emergence. Despite these barriers, we know more about prevention than most people in Homeland Security are aware of. The *Preparedness Guidelines for Homeland Security*, issued in 2003 by the DHS, identifies five elements of a cohesive prevention strategy: collaboration, information sharing, threat recognition, risk management, and intervention. These *Guidelines* provide a good initial framework for effective prevention. We can continuously improve the *Guidelines* by transforming them from a proprietary to an "open source" project within the public safety community.

AUTHOR BIOGRAPHY: Christopher Bellavita teaches in the Masters Degree program at the Naval Postgraduate School in Monterey, California. An instructor with twenty years experience in security planning and operations, he serves as the Director of Academic Programs for the Center for Homeland Defense and Security. Prior to joining NPS, Dr. Bellavita was the executive director of the Utah Olympic Public Safety Command. He received his Ph.D. from the University of California, Berkeley.

KEYWORDS: bias towards response, fear of new behaviors, fear of imagination, fear of emergence, collaboration, information sharing, threat recognition, risk management, intervention, Preparedness Guidelines

"I don't think you can win [the war on terror]."
– George W. Bush

"He was talking about winning it in the conventional sense ... about how this is a different kind of war and we face an unconventional enemy."
– White House spokesman Scott McClellan[1]

May 20, 2005 passed with little notice in America. It marked 1,347 days since the September 11th attack. The same number of days separated December 7, 1941 from the end of the Second World War. This "different kind of war" will not end. There is no politically palatable way for a leader to say, "OK, we won. The Global War on Terror is over. Everyone go back to Green."

Like its semantic relatives the War on Drugs and the War on Poverty, the Terrorism War will last as long as there are homeland security industries, bureaucracies, and congressional committees. And an enemy. There is no war on terrorism without terrorists – considered now, under U.S. law and sentencing guidelines, as anyone whose action "appears to be intended to intimidate or coerce a civilian population."[2] Since a terrorist can include criminals who fly planes into buildings, detonate bombs at sporting events, set SUVs on fire, release laboratory animals, and make methamphetamines, we will never run out of terrorists.

PREVENTION REMAINS OUR FIRST NATIONAL PRIORITY

Because we are in this for the long run, it is important to remember what we are trying to accomplish. The National Strategy for Homeland Security published in 2002 identifies prevention as the first of four goals. In April, 2005, Department of Homeland Security (DHS) Secretary Michael Chertoff reaffirmed the importance and priority of prevention when he told Congress our homeland security strategy was to keep terrorists "off the boards, prevent them from coming in, prevent them from shipping their stuff in, protecting our infrastructure and transportation if they do get in, and then if worse comes to worst, … being able to respond the *[sic]* mitigate the harm."[3] In word, if not in deed, prevention remains our first priority.

After more time than we devoted to Word War II, how are we doing? We have not been attacked in almost four years. By the end of 2005, we will have spent about 175 billion dollars on homeland security. Information sharing, while not perfect, has dramatically improved – at least among law enforcement agencies. We have a dozen homeland security-related national strategies; fifty-plus state and territory strategies; thirteen homeland security presidential directives; and a growing mound of implementation guides, cloaked by such New Deal-sounding acronyms as NRP, NIMS, NPG, NIPP, UTL, and TCL.

On the surface, our prevention strategy is working. Look under the surface however, and one is hard pressed to identify what that prevention strategy is.

HAS ANYONE SEEN THE TERRORISM PREVENTION PLAN?

> *The Committee is concerned that while terrorism prevention is a national priority, little is being done to create prevention expertise in our nation's first responders. This is in stark contrast to response and recovery training programs. Without a well-developed terrorism prevention plan, State and local agencies lack a key piece in the fight against terrorism.*
>
> – House Appropriations Subcommittee on Homeland Security, June 2004 [4]

Imagine a parallel universe where World War II is still going on. There is a strategy meeting in President Roosevelt's office. The Director of the Office of Civilian Defense is speaking:

"When the German's attack, Mr. President, here's how we'll be organized. We will use the National System for Managing Any Incident…."

"Wait," says the President, "First tell me how we will prevent the Germans from attacking."

"Well," says the Director, "our National System for Managing Any Incident has a strong prevention component. Everyone will work together and share information. But once we're attacked…."

"Stop. How do we prevent the attack in the first place?"

"Mr. President," says the Director, "You'll recall we have a National Response Plan, and…."

"I don't want to respond," says the President. "I want to prevent."

"The country has not been attacked since December 7th, Mr. President. And the Germans have never attacked our homeland. Our plans are working."

Almost four years have gone by since the nation formally joined the global war on terrorism. Yet something still is preventing us from giving as much – if not more – attention to prevention as we give to preparing to respond to the next attack.

One reason is money. The political economy of homeland security is biased toward response. A lot of money has been made selling equipment and services to first responders. There is a much more limited economic market for prevention. We do not know how much we are spending on prevention because we do not yet have a common understanding of what we do when we are preventing terrorism.

The Homeland Security Appropriations Subcommittee quotation, above, alluded to a "terrorism prevention plan." What is that? Where is it? Why is it taking so long to put together? What is preventing homeland security from preventing terrorism?

IT IS THE SYSTEM, NOT THE PEOPLE

> *"We've got to have a prevention strategy that is focused on finding those terrorists before they act. Very little, I will hasten to add, of what the Department of Homeland Security spends its money on these days is devoted to what ought to be a high priority. We've got to reconfigure in order to do that."*[5]
>
> – Christopher Cox, [Former] Chairman of House Committee on Homeland Security

It would be completely erroneous to say we do not have comprehensive national or local prevention plans because no one wants them. It would be foolish to blame any person or institution for the failure to make prevention the first priority in more than name only. There are many people at all levels of government who take with heart attack seriousness the prevention mission. But we have been at this longer than WWII, and we still do not have a cohesive – or articulated – national prevention strategy. Something is wrong.

Edwards Deming, the continuous improvement authority, used to say, "We are being ruined by the best efforts of people who are doing the wrong thing." To Deming, systems rather than people were the problem. "All that happens comes from the system, not the workers…," he said. "It's absolutely frightening, … just frightening."[6]

The same dynamic is festering in homeland security: the best efforts of the best people are being applied to the wrong things. As Christopher Cox, former Chairman of the House Committee on Homeland Security suggests, the homeland security system is not designed to support prevention as its first priority. It is designed to respond. It is leadership's job to reconfigure the homeland security system, to make the system's outputs conform to the priorities of our national strategy.

"Reconfiguring the system" does not mean simply reorganizing the Department of Homeland Security. A secure homeland is the outcome of national, state, local, private sector and citizen activities. It is not the sole responsibility of any national, state or local agency.

Deming argued for the preeminence of process. If you understand system processes, he said, you can figure out what needs to be done to continuously improve that system. Before trying to redesign the entire homeland security apparatus, however, it may be helpful to examine three systemic fears that get in the way of discovering how the activities of that system – the process – can match the espoused priority of prevention. They are the fear of new behavior, the fear of imagination, and the fear of emergence.

THE FEAR OF NEW BEHAVIOR

In late 2004, public safety executives from a mid western state participated in a homeland security tabletop exercise. The first scenario was designed to stimulate conversation about how to prevent a potential attack from happening. The discussion was low energy and uninspired. Participants were unsure how to talk about prevention.

But then an attack scenario was presented. The exercise moved into response and recovery. Participants became animated. They talked faster, had more detailed

knowledge, and were professionally confident. They demonstrated they knew what to do once an incident has happened.

The same pattern was repeated in more than a dozen similar state homeland security exercises: people participating in the exercises could not grab hold of "prevention" with the same emotion they poured into "response." The reason? The public safety leaders had a lot of experience responding to critical incidents. They had practically no experience sharing at least awareness that they were doing prevention.

New Roles, New Behaviors

Preventing terrorism is a new role for public safety agencies. They are used to responding to daily emergencies, not stopping acts of war. As a generalization, one can say they tend to avoid prevention because they already know how to do response. It is partially a learning problem. Adults and organizations prefer doing things they already know how to do – even if that means redefining the "new" so it looks like the old; hence the demand for new and better response equipment – whether or not it can be used or maintained.

The United States has the world's best disaster response system. With the possible exception of a wide scale biological or cyber attack, we can meet the challenge of any incident – no matter how horrendous. That does not mean we have finished improving our response system. But continuing to make response our de facto priority is like searching for lost car keys under a street light because the light is better there. We know much less about how to prevent. It is in this Terra Incognito we can make the most progress expanding our capability to secure the homeland.

We have a Roadmap for Prevention

While prevention may be a new public safety idea, we know more than most people in homeland security are aware of. In 2003, the DHS issued *Preparedness Guidelines for Homeland Security*. The *Guidelines* have three features that make it unique among the paniculated documents produced since September 11th. It was built from the ground up by first preventers. It was vetted by first preventers. It gave other public safety professionals practical advice about how to prevent terrorism. For some reason, the *Guidelines* are also largely unknown in the homeland security community.

The *Guidelines* identifies five elements of a prevention strategy: collaboration, information sharing, threat recognition, risk management, and intervention. Each of these elements is further divided into specific activities that support the prevention strategy. The two core elements of those *Guidelines* – collaboration and information sharing – cost comparatively little in monetary terms. They mostly require people, organizations and professions to change their attitudes and behaviors. The core elements work only when there is a committed effort to change. Their success is more a function of sociology than technology.

The *Guidelines* can be a foundation for developing local prevention plans. Some jurisdictions – in Kansas City, KA and Frederick County, MD, for example – have already used the *Guidelines* this way.

The *Guidelines* also can help with the thorny problem of how to measure prevention. The prevention activities included within each of the five elements are empirically

derived proxies for prevention. If the elements are present and working effectively in a jurisdiction, there is a greater likelihood a process is in place to prevent terrorism.

The *Prevention Guidelines* – or something similar – are as important to homeland security as the National Incident Management System (NIMS). The national government threatens to withhold funds to jurisdictions that are not "NIMS compliant." If prevention is so important, the Grant Threat strategy could be extended to agencies – and the private sector (perhaps with what amounts to a tax penalty) – that are not "prevention compliant." The *Prevention Guidelines* make concrete what it means to prevent terrorism.

THE FEAR OF IMAGINATION

The 9/11 Commission Report cited the failure of imagination as one of four failures revealed by the attack. The post 9/11 spending hemorrhage has fertilized imaginative technology – although there is no evidence the absence of technology contributed significantly to the September attacks. At the national level, there have been no especially imaginative innovations in policy, strategy or how we are organized to prevent terrorism. The NIMS is a modification of a thirty-year-old template for responding to emergencies. The lackluster "Vision for the National Preparedness Goal" reads like a "what-not-to-do" example in a government writing class. Merging 22 agencies into one is – although on a major league scale – a traditional organizational response to not knowing for sure what to do.

If this truly is, as presidential spokesman Scott McClellan asserts, "a different kind of war," we are still fighting it with old ideas, old structures, and old methods. Four years and counting. Where is the imagination that the 9/11 Commission called for? Here are two ideas: confront the American people with the reality of what terrorism can do to our society, and use free market ideas to predict the risk of specific attacks.

"… nameless, unreasoning, unjustified terror"

Prevention has to mean more than just stopping attacks. It also ought to mean preventing terrorists from achieving the goals their attacks are meant to accomplish. How would Americans react economically, politically, and socially if twenty suicide bombs went off within the same hour in shopping malls all over the country? What if smallpox starts to show up? Or if transit systems in our cities are attacked like London's or Madrid's? What if car bombs start detonating in American cities with the frequency they explode in Iraq? What happens if an airplane is shot down as it takes off from an American airport?

It would cost about 40 billion dollars to install missile defense systems on the nation's commercial air fleet over the next two decades to protect against shoulder fired missile attacks. Experts are split over the likelihood of such an attack. But there is general agreement that the central justification for even considering such an expenditure is because "of the enormous economic consequences that would result if the public were to lose confidence in flying.[7]" The terrorist target is not the airplane, or the mall, or the subway. Bin Laden has made his goal clear. The target is our economy: "We bled Russia for ten years until it went bankrupt and was forced to withdraw in defeat…. We

are continuing in the same policy to make America bleed profusely to the point of bankruptcy."[8]

Thomas J. Housel and Arthur H. Bell argue, in "Limiting the Impact of Terrorist Acts: Accessing the Wisdom Base of a Hardened U.S. Populace," that theAmerican people are insufficiently prepared to prevent the economic and social disruption such an attack would create.[9] History teaches that people as well as critical infrastructure can be hardened against terror. If the enemy wants to wreck our economy by making people afraid to take the subway or go to malls, part of our approach to prevention should be to undercut the power of the terrorist strategy by toughening people against what is likely to happen again in our lifetime. If we are in a real, not a symbolic, war, men and women and children will die. Trying to protect Americans from that truth – as we do with the casualties of the Iraq war – eviscerates one of the fundamental weapons in our prevention arsenal.

Stephen Flynn suggests we are in a "phony war" period similar to the eight months after the Germans invaded Poland in September 1939. Read or listen to what Winston Churchill told the British people: "I have nothing to offer but blood, toil, tears and sweat." His prediction was correct, but the residents of London went on with their lives in spite of daily Luftwaffe air raids. Compare that to the fuzzy way we have prepared American citizens for the next attack – and for what they can do about helping to prevent the attack and – more importantly – the consequences of an attack.

Placing Bets on the Second Attack

The most imaginative strategic idea for fighting terrorism we have so far seen was the Policy Analysis Market (PAM), incorrectly known as "terrorism futures." It was designed to use speculative markets to forecast geopolitical trends. People who did not know what they were talking about perceived it as a way to bet on terrorist attacks.[10] The PAM was an effort to create decision markets about the potential consequences of policy actions. It was premised on the assumption that markets are efficient and effective aggregators of information. Empirically, markets do a better job of assessing risks than reports or experts. It does not get much more American than calling on free market concepts to help prevent terrorism.

But what a ruckus this new idea caused. It was cancelled one day after the project came to the attention of the mainstream press. One might debate the pros and cons of decision markets as a way to look at prevention policies. But that debate never happened. Do we have such a surplus of ideas that we are incapable of withholding judgment long enough to listen to what the idea is before it is killed? What other innovative ideas about policy, strategy, and organization have been blocked by homeland security mind guards?

If public sector decision markets prove to be an advance on our current policymaking capabilities, homeland security will eventually adopt them. But who knows how much time will go by – how many questionable decisions made – before then. In theory, some of the initial stakeholder confusions and disagreements over NIMS, the Target Capabilities List, and other DHS efforts could have been minimized if decision futures markets would have been encouraged to weigh in. But we will never know.

The larger problem is not how the DHS writes rules. It is a system-wide bias against imagination. This can be addressed, in theory, by a commitment to "seek first to understand" ideas before killing them. Perhaps a small reserve of seed funds could be

used for "imagination grants." These would be provided to communities, states, the private sector, and national government agencies – anyone who has an inventive and intellectually plausible idea about how to expand our capacity to prevent terrorism.[11]

The 9/11 Commission called for institutionalizing imagination. That has not yet been done. It needs to be.

THE FEAR OF EMERGENCE

> *During the past three years, many federal agencies … have made efforts to secure input and comments from the state, tribal, and local public safety community. Unfortunately, these efforts are too often limited to participation in advisory panels and working groups that have little impact on policy development and instead are relegated to the role of providing post-development comments on completed, or nearly completed, policy proposals. Consequently, the ability of state, tribal, and local law enforcement to truly influence policy has been minimized.*[12]

The third fear is the dread of what happens if you stop trying to control everything. It is based on a proposition demonstrated by experience time and again: control is not a property of complex human systems. The social, political, and economic world is not a product of control. It is the resultant of an emergent, self-organizing process.[13] That does not mean homeland security professionals play no role in shaping the system. But they are partners, not controllers. Homeland security leaders can benefit from transforming their thinking from a hierarchical to a network mindset.

Envision the textbook pyramid of "How Our Government Works:" the national government is on top, telling the states what to do to the cities and counties. Using the relatively new policy mechanism of the "presidential law," otherwise known as Homeland Security Presidential Directives (HSPD), the national government now tells states and cities what they need to do to secure the homeland. States and cities have allowed this to happen for a variety of reasons – ranging from the perception that homeland security is little more than a way to get grant funds, to the authentic belief that it is the national government's job to set the homeland security agenda.

The national government, partly through default, partly through arrogance, and partly because of the career history of institutional leaders, has welcomed the opportunity to decide what is best for homeland security. Most homeland security guidance documents are the product of this hierarchical mentality. From the National Strategy through the HSPDs and the follow-on suite of implementation documents, the national government has been telling its subordinate units what to do.

Because this is the 21st century, however, it is symbolically necessary to get "input from the locals." But as recent reports from the International Association of Chiefs of Police, the Government Accountability Office, and the Congressional Research Service indicate, the well-meaning efforts at inclusion are largely unconvincing to those on the frontlines of homeland security.[14]

The dominant metaphor driving homeland security aspirations is "the well-oiled machine," steered by an informed central authority. It is based on the theory that if all

the parts – states, cities, private sector, citizens, and the national government agencies – are operating from the same design (e.g., the NPG, NRP, NIMS, TCL, and so on) we will have one integrated system that will achieve the national homeland security strategy.

There are two problems with the metaphor and with the behavior it encapsulates. First, the machine is not designed to do what it should do: prevent terrorism. It is designed predominantly to create and follow rules, and to spend money for response. Second, the exclusionary faith in hierarchy and control sustains a societal vulnerability our enemy has already exploited.

The enemy is networked. We are too, although we could get much better at it.[15] Most people in homeland security know that the way things really get done is through personal networks. But we still talk and act as if a smoothly functioning hierarchy ought to be our goal; blindly maintaining this almost-vestigial twentieth century idea gets in the way of preventing terrorism.

DHS policy says that money should go directly to states, to then be distributed to cities. Politically powerful communities have found ways of effectively bypassing states and going directly to DHS, at times via Congress, at other times by creating the right relationships with DHS and other agency leaders. Funding is as much the product of networks, as of hierarchies.

Review the collection of recent state homeland security plans.[16] Many of these plans were spurred by rather explicit DHS grant guidance. Yet there is extraordinarily wide variation in the plans. The best explanation for why plans were written as they were rests in understanding the network of people and agencies responsible for the plan, not the guidance from the national government.

Monitor how states and cities and counties will implement NIMS. For some communities, NIMS represents a modest extension of what they already are doing. For others it represents a welcome lever to get all agencies to use the incident management system. For still others, it represents yet another intrusive mandate to be worked around. One can predict that the future of NIMS will be the resultant of the same network processes that helped to shape the funding and the planning profiles. It will not be controlled by the national government – not because control is or is not a good idea, but because control is not a property of a complex human system like homeland security.

This is not an argument to eliminate hierarchy. It is a suggestion that since the present system is having such a difficult time pursuing prevention, try something different. Instead of struggling to control what happens in homeland security, use the power of self-organization to see what it can contribute to expanding our prevention capabilities. Use the creativity of communities, states, the private sector, and homeland security professional associations to evolve the next iteration of the *Prevention Guidelines.* Here is how that might work.

First the theory: Many DHS documents talk about the need for policies and strategies to "evolve" as time goes by.[17] "Evolve" is in quotes to emphasize that it has a meaning beyond the general one of "change." From a theoretical perspective, the evolutionary process is quite specific: it includes variation, selection, and reproduction.[18] The first requirement is for variation. The homeland security system already has lots of that – in spite of efforts to minimize unplanned variation. Another word for "selection" is "best practices" (or, more accurately, "smart practices"[19]). If there is an effective process for sharing smart prevention practices, it is informal and underground. It is possible to

develop a mechanism – beyond the DHS Lessons Learned website (www.llis.gov) – that targets a specific set of prevention ideas for possible selection by agencies willing to experiment. The next step is for jurisdictions to adopt – or reproduce – particular smart practices that do work in their environment. This is a naturalist rather than a mechanical model. It is relying on intelligent, co-evolution rather than on intelligent design by committee.

Now the practice: The co-evolutionary approach does not require developing any new implementation strategy. Instead, it represents taking the blinders away to see what is actually happening – networks are organizing homeland security, not hierarchies – and then cooperating with the reality of how things happen, rather than remaining faithful to an ideal about controlling complexity.

Possibly the best example of co-evolution in homeland security is fusion centers. They were not mandated. It just seemed like a good idea that agencies with something to contribute to situation awareness ought to talk with each other. That "variation" of the pre 9/11 compartmentalized intelligence structure was voluntarily selected and voluntarily reproduced by other states and communities.[20]

The target for the self-organizing experiment would be the DHS *Prevention Guidelines.* The 2003 *Guidelines* are not the last word in prevention. They need to be continuously improved as we learn more about what works. In early 2005, a draft Version 2 of the *Guidelines* was released by DHS – but then subsequently withdrawn. The DHS Lessons Learned web site could post the *Guidelines* as a "wiki" to allow broad input into the continuous improvement of what works in prevention.[21]

The idea is to make the *Prevention Guidelines* an "open source" rather than a proprietary project within the public safety community. It is analogous to the development of the Linux computer operating system, where "Given enough eyeballs, all bugs are shallow".[22] We should foster as much variation of the *Prevention Guidelines* as possible. Individual agencies would be encouraged to take the guidelines, adapt them to their jurisdiction, and add what they learn to the *Guidelines*.[23] Let the public safety market of ideas determine what can be done at state and local levels to prevent terrorism.

There have been endless documents produced by committees working inside cathedrals of homeland security orthodoxy. Let us discover if the revised guidelines for preventing terrorism can organize itself, using the wisdom of the "great babbling bazaar of differing agendas and approaches" that makes up homeland security.[24]

---

[1] Julian Borger, "President admits war on terror cannot be won," *The Guardian*, August 31, 2004. http://www.guardian.co.uk/international/story/0,,1293965,00.html [Accessed May 15, 2005]

[2] U.S. Code: Title 18, Part I, Chapter 113b, Sec. 2331. See also, George Bush, Executive Order 13224, September 24, 2001.

[3] Testimony by Secretary Michael Chertoff before the House Homeland Security Committee, Washington, D.C., April 13, 2005. Accessed June 12, 2005 at http://www.dhs.gov/dhspublic/display?content=4460

[4] Committee Report accompanying the *Department Of Homeland Security Appropriations Bill, 2005,* H.R. 4567. http://thomas.loc.gov/cgi-bin/cpquery/T?&report=hr541&dbname=cp108& [Accessed June 12, 2005]

[5] Chris Strom, "Lawmaker challenges companies to develop anti-terror technology," *Daily Brief*, Govexec.com, May 25, 2005. http://www.govexec.com/dailyfed/0505/052505c1.htm [Accessed May 27, 2005]
[6] Carla Lazzaresche, "In Endless Pursuit: A Hero in Japan, Deming Continues His Quest for Quality at Home," *Los Angeles Times*, December 5, 1993.
[7] Eric Lipton, "U.S. Is Set to Test Missile Defenses Aboard Airlines," *New York Times,* May 29, 2005. http://www.nytimes.com/2005/05/29/national/29missiles.html [Accessed June 1, 2005]
[8] Gal Luft, "Al Qaeda's economic war against the United States," *Energy Security*, January 24, 2005. http://www.iags.org/n0124052.html [Accessed May 28, 2005]
[9] Thomas J. Housel and Arthur H. Bell, "Limiting the Impact of Terrorist Acts: Accessing the Wisdom Base of a Hardened U.S. Populace," March 2005 (unpublished).
[10] Robin Hanson, "The Informed Press Favored the Policy Analysis Market," Department of Economics, George Mason University, May 5, 2005. http://hanson.gmu.edu/policyanalysismarket.html [Accessed May 19, 2005]
[11] Imagination grants would not duplicate the goals of the Homeland Security Centers of Excellence program. They would, instead, be short-term, small budget expenditures designed to support a skunk works type exploration of innovative ideas. For an example of a prevention-related idea worth exploring through an imagination grant, see the discussion of using "smart mobs" for homeland security at http://www.techcentralstation.com/021403A.html, and http://stephensonstrategies.com/stories/2004/09/29/10pointPlanToMakeSecurityM.html. Smart mobs are groups that use technology to behave intelligently or efficiently. Smart mobs could be used to augment public safety eyes and ears on transportation systems, at major events, and other public sites.
[12] International Association of Chiefs of Police, "From Hometown Security to Homeland Security," May 17, 2005:5-6.
[13] Steven Johnson, *Emergence* (New York: Touchstone, 2001) and Albert-Laszlo Barabasi, *Linked* (Cambridge, MA: Perseus Publishing, 2002).
[14]International Association of Chiefs of Police, "From Hometown Security to Homeland Security," May 17, 2005. Congressional Research Service, "The National Preparedness System: Issues in the 109th Congress," March 10, 2005: 29 30. U.S. Government Accountability Office, "Homeland Security: Much is Being Done to Protect Agriculture from a Terrorist Attack, but Important Challenges Remain," GAO report GAO-05-214 (Washington: March 8, 2005): 47 48.
[15] John Arquilla, David Ronfeldt (eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (RAND, 2001).
[16] For examples, see the Memorial Institute for the Prevention of Terrorism collection of state homeland security strategies at http://www.mipt.org/State-Homeland-Security-Plans.asp. Some have noted that many of the "plans" seem to be more concerned with how money will be spent than with what the state's homeland security strategy will be.
[17] *The Interim National Infrastructure Protection Plan* (Department of Homeland Security, February 2005), for example, talks about evolution more than a dozen times.
[18] For a review of the argument linking evolutionary theory to contemporary organizational issues, see Lawrence and Nohria, *Driven: How Human Nature Shapes our Choices* (Jossey-Bass, 2002).
[19] For the significant difference between best practices and smart practices, see Bardach, *A Practical Guide for Policy Analysis* (Chatham House, 2000).
[20] As of June 2005, six states had working fusion centers; another dozen states were in the process of developing them. See National Governor's Association, "Intelligence Fusion Center TA Request," June 2005 for a status report on state involvement with fusion centers. For another example of a multi-agency approach to collaboration that emerged from need rather than edict, see the Pasadena, Texas police department's Community Defense Unit, at http://www.ci.pasadena.tx.us/police/operations/CDU/CDU.htm.
[21] Wiki is an abbreviation for "What I Know Is." Wiki is a process that is used in collaborative networks on a website (or other hypertext document collection) that allows users to add content, but also allows anyone to edit the content.

[22] Eric S. Raymond, "The Cathedral and the Bazaar," *First Monday*, March 1998, http://www.firstmonday.org/issues/issue3_3/raymond/ [Accessed 1 June 2005]. Translated from computer talk, the quote suggests the more people who review something, the easier it is to find errors. James Surowiecki, in The Wisdom of Crowds," (Doubleday, 2004) makes a similar point. He applies the self-organizing/emergence logic to decision-making and decision markets and notes four conditions that have to be met before the judgments of many individuals are likely to be superior to expert judgment: diverse opinions, independence, decentralization and aggregation. All four conditions could be met in the experiment suggested here.

[23] Thomas J. Dailey, "Implementation of Office for Domestic Preparedness Guidelines for Homeland Security Prevention and Deterrence June 2003" (master's thesis, Naval Postgraduate School, Center for Homeland Defense and Security, March 2005).

[24] Eric S. Raymond, "The Cathedral and the Bazaar."