Color Bind

Lessons from the Failed Homeland Security Advisory System

Jacob N. Shapiro and Dara Kay Cohen

From its inception in 2002, the color-coded terrorist alert system known as the Homeland Security Advisory System (HSAS) has been both the U.S. government's most visible domestic counterterrorism tool and the brunt of endless jokes and derision. Underlying these comic insults, however, remain serious questions about the system: Does it work? If not, what are the central problems? And how might these problems be eliminated, or at least mitigated, in an alternative system? In this article, we argue that compliance with a terrorist alert system must be based on confidence in the value of the information it provides. The HSAS was not designed to generate such confidence; rather, its designers assumed that the public would trust the national leadership and believe in the utility of the system's information. Over time, as the system became increasingly perceived as politically manipulated, there was no built-in mechanism to recover lost confidence, and as a result the HSAS has failed.

An effective terrorism alert system has one central task: to motivate actors to take costly protective measures. In the United States, national leaders do not have the statutory authority to order specific actions from constituent governments and private industry. Instead, the federal government must convince them that the desired actions are worthwhile. Conditional on an alert being issued, these actors must believe that the costs of protection are less than the expected losses of not providing protection. Such beliefs can be generated in one of two ways: the government can share specific threat information to motivate protective action, or it can generate enough confidence in the alert system that its word alone sufficiently increases actors' beliefs about the probability of an attack that they willingly take the desired actions.

The HSAS does not provide enough information to the actors involved and contained no mechanisms to generate confidence in the system over time. Consequently, it came to be deeply mistrusted. In August 2004 a survey found

Jacob N. Shapiro is a postdoctoral fellow at the Center for International Security and Cooperation (CISAC) at Stanford University. Dara Kay Cohen is a Ph.D. candidate in political science at Stanford University. She wrote this article as a predoctoral fellow at CISAC.

The authors thank James Breckenridge, Rudy Darken, Laura Donohue, Lynn Eden, Michael May, Terry Moe, Charles Perrow, Scott Sagan, Paul Stockton, Barry Weingast, and the anonymous reviewers for their helpful comments and criticism. They are especially grateful to the Center for International Security and Cooperation for supporting this research. They also wish to thank Jacob Shapiro's students at the Center for Homeland Defense and Security and the other homeland security officials who took the time to help them, many of whom asked to remain anonymous.

International Security, Vol. 32, No. 2 (Fall 2007), pp. 121–154

that fully 38 percent of likely voters believed that the alerts might be used for political reasons.[1] The HSAS had become so widely unpopular that in 2004, Democratic presidential candidate John Kerry promised to abolish it if elected.[2] While the public derision and scholarly criticism of the HSAS highlight the failure to generate public confidence in the system, they also contributed to that failure. Once the system began to lose credibility, the media treated it less seriously, further eroding its credibility and producing a self-reinforcing cycle. This dynamic contributed to significant levels of noncompliance with the HSAS, ultimately leading to the current state: its complete marginalization by the constituent governments and the public. The problems inherent in the now failed HSAS have not been addressed in any of the existing critiques, which tend to focus on how the HSAS deviates from the best possible systems for disaster warning and counterterrorism alerts.[3]

In this article, we discuss both the failure of the HSAS and the broader logic of terror alerts in a federal system of government. We identify a causal chain of events that must occur for any such system to be successful and argue that because of the strategic environment for terror alerts, the links in this chain are much stronger if confidence in the system is actively employed, rather than assumed, to motivate protective actions. Drawing on political science, organization theory, and psychology to inform our argument, we propose an alternative system that solves several major flaws in the current system. Our proposal draws particularly on the notion of "procedural fairness," which suggests that people are much more likely to follow orders from a central authority if they believe that authority has used a just process to make its decisions.

This alternative system corrects the main problem that HSAS has experienced in motivating protective actions—the lack of trust in the value of the alerts—by requiring the federal government to prenegotiate a set of measures available at each alert level with private industry and constituent governments. This requirement would ensure that the system would be sufficiently specific about the nature of the threat and the actions to be taken. That sense of value, combined with the trust developed during the negotiations, would

1. "Voters Unmoved by Terror Alerts," *Time.com,* August 6, 2004, http://www.time.com/time/election2004/article/0,18471,678367,00.html.
2. Corbett Riner, Liza Porteus, and Mike Emanuel, "Trail Tales: Color Code Conundrum," *FoxNews.com,* October 21, 2004, http://www.foxnews.com/story/0,2933,136190,00.html.
3. See, for example, Stephen Flynn, *America the Vulnerable: How Our Government Is Failing to Protect Us from Terrorism* (New York: HarperCollins, 2004); Kenneth Allen, "The Homeland Security Advisory System: Threat Codes and Public Responses," testimony before the House of Representatives Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, 108th Cong., 2d sess., March 16, 2004; and Lawrence Freedman, "The Politics of Warning: Terrorism and Risk Communication," *Intelligence and National Security,* Vol. 20, No. 3 (September 2005), pp. 379–418.

greatly enhance confidence in the system. This alternative system would allow for more precise, more predictable responses from federal, state, and local agencies and, most important, would enhance the system's ability to generate the federal government's desired protective measures.

The remainder of the article proceeds as follows. The first section describes the Homeland Security Advisory System, examines its origins, and outlines its gradual failure. The second section briefly explores terrorism alert systems in other nations. The third section examines the logic and purposes of terror alerts. The fourth section analyzes three key weaknesses of the HSAS. The fifth section develops our alternative system and identifies why it is preferable to the HSAS.

The Rise and Fall of the HSAS: A Critical Review of Recent History

At a press conference six months after the September 11, 2001, terrorist attacks, former Governor Tom Ridge of Pennsylvania, then director of the White House Office of Homeland Security (OHS), announced the creation of the color-coded HSAS. Following on the March 12, 2002, announcement, the White House issued Homeland Security Presidential Directive 3 (HSPD-3) outlining the system. HSPD-3 applies to all federal "facilities, personnel, and operations inside the territorial United States [and] all Federal departments, agencies, and offices other than military facilities."[4] Its stated goal is to "reduce vulnerability or increase response capability during a period of heightened alert."[5]

The system, which became the government's most prominent domestic counterterrorism tool, has five threat levels, each corresponding to a particular color: low (green), guarded (blue), elevated (yellow), high (orange), and severe (red). HSPD-3 describes "risk" as including both the probability of an attack occurring and its potential gravity. Importantly, these criteria are silent on what a "high risk" or a "severe risk" actually entails. This lack of explicit criteria is in stark contrast to older homeland security documents such as the January 2001 United States Government Interagency Domestic Terrorism Concept of Operations Plan—superseded in December 2004 by the National Response Plan—which contained detailed descriptions of what types of intelligence would trigger each level of alert. In the absence of information about the trustworthiness of a particular authority, people react more favorably to—and

4. "Homeland Security Advisory System," Homeland Security Presidential Directive 3, March 11, 2002, http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html.
5. Ibid.

are therefore more likely to comply with—an authority's actions when they believe that authority uses fair procedures.[6] Because it provides no information about the procedures behind its alert levels, or about the intelligence requirements for them, the HSAS has not generated many favorable reactions. State agencies have tried to fill this gap with more detailed subsidiary guidelines,[7] sometimes containing criteria that conflict with HSPD-3.[8] The lack of clarity as to what the color levels require is one of the major weakness in the HSAS.

A further issue with the HSAS is uncertainty regarding what it actually includes. At its inception, the HSAS consisted solely of the color-coded alert system, at least according to HSPD-3. Two other elements were added later. On the website of the Department of Homeland Security (DHS), the agency states that the HSAS consists of the following elements: (1) homeland security threat advisories, which are warnings to state and local governments that are supposed to contain actionable information about specific threats; (2) homeland security information bulletins, which contain information regarding critical infrastructures that does not warrant a specific warning, but that the government still restricts to state and local governments; and (3) the "Color-coded Threat Level System," which is "used to communicate with public safety officials and the public at large through a threat-based, color-coded system so that protective measures can be implemented to reduce the likelihood or impact of an attack."[9] Nevertheless, the HSAS has been mainly understood by the public, local governments, portions of the federal government, and academics to include only the color-coded component. Our critique therefore centers on this part of the system.

The three-component system, with its public tiered warning system and private, government-only threat advisories and information bulletins (each with different objectives and modes of operation), sounds laudable. The threat advisories, however, do not appear to provide actionable information (at least not those that have been made public). For example, Alert 03-025, which accompanied the May 20, 2003, orange alert, announced that "intelligence reports in

6. Kees van den Bos, Henke A.M. Wilke, and E. Allan Lind, "When Do We Need Procedural Fairness? The Role of Trust in Authority," *Journal of Personality and Social Psychology,* Vol. 75, No. 6 (December 1998), pp. 1449–1458.
7. Commonwealth of Kentucky Department of Military Affairs, "Readiness of the Commonwealth to Respond to Acts of War or Terrorism, 2003 Annual Report," p. 58.
8. Washington Military Department, *Guidelines for the Implementation of the State of Washington Homeland Security Advisory System,* February 31, 2003, p. 6; and State of Louisiana Military Department, *Louisiana Homeland Security Strategy,* March 31, 2003, pp. 60–64. For a collection of state homeland security plans, see National Memorial Institute for the Prevention of Terrorism, http://www.terrorisminfo.mipt.org/State-Homeland-Security-Plans.asp.
9. Department of Homeland Security, "Homeland Security Advisory System," http://www.dhs.gov/xinfoshare/programs/Copy_of_press_release_0046.shtm.

recent months point to a wide range of possible infrastructure targets that Al-Qa'ida may have plans to attack. These include key assets, such as nuclear power plants, dams, and government facilities; the energy sector, to include power-generating facilities, fuel farms, and gas stations; the transportation sector, to include passenger rail, freight trains carrying toxic industrial chemicals, civil aviation, rail and vehicle bridges, tunnels, [and] subways; [and] direct attacks on financial institutions."[10] The actions for businesses included suggestions such as "[c]onsider installing telephone caller I.D., record phone calls, if necessary," hardly what one imagines an organization doing in response to actionable threat information. Later advisories, such as the yellow-to-orange August 1, 2004, advisory for the financial sectors in New York, New Jersey, and Washington, D.C., were more specific.[11]

Because the advisories have been redacted before being made public, it is impossible to know if they contained recommended actions linked to more specific threats. What is known is that these private components of the HSAS do not provide as much information as local officials feel they need. A survey for the Gilmore Commission Report—the final product of a congressional advisory panel, convened from 1999 to 2003, on domestic responses to potential attacks of terrorism with weapons of mass destruction—found that 60 to 80 percent of local and state organizations wanted more specific information on the type of incident, location, and time period of the threat.[12] This was not simply a learning problem in the system's early stages. In 2005 the Government Accountability Office (GAO) reported that even federal agencies, which presumably receive all the private threat advisories, were unable to determine appropriate protective actions because of the lack of specific threat information.[13]

Although it is not clear when the threat alerts and information bulletins were added as official components of the HSAS, it is obvious they are not generally understood to be part of the system.[14] Many state homeland security de-

---

10. Department of Homeland Security, "Alert 03-25," http://www.dhs.gov/interweb/assetlibrary/Threat_Orange_052003 (accessed April 21, 2006; site discontinued).
11. Department of Homeland Security, "Homeland Security Advisory System Increased to ORANGE for Financial Institutions in Specific Geographical Areas," http://www.dhs.gov/interweb/assetlibrary/IAIP_AdvisoryOrangeFinancialInst_080104.pdf (accessed April 21, 2006; site discontinued).
12. Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission), "Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty," *Fifth Annual Report to Congress* (Arlington, Va.: RAND Corporation, December 15, 2003), p. D-7-2, http://www.rand.org/nsrd/terrpanel/.
13. GAO, *Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security,* GAO-05-33 (Washington, D.C.: GAO, January 2005), p. 40.
14. A distinction between the public system and the private threat advisories and information bulletins first appears in a February 2004 GAO report, but the advisories and bulletins are treated as something separate from the HSAS system. GAO, *Homeland Security Advisory System: Preliminary*

partment websites do not discuss the two components when describing the system.[15] GAO reports do not mention either by name, even when discussing DHS's information-sharing practices, and describe the system as "requir[ing] that terrorism threat alerts be issued to the public."[16] Nor do the few academic analyses of the system mention them.[17] And, most notable, many homeland security officials do not recognize them as part of the HSAS.[18] Moreover, assessing the efficacy of the nonpublic components of the system is impossible given the small number of threat advisories and information bulletins that have been made public and the reticence of state and local officials to speak on the record about their experiences with them.[19]

The federal government has many ways, both formal and informal, to try to motivate protective actions by constituent governments and private entities.[20] Our analysis focuses on the narrower question of whether a tiered public warning system, designed and used as the HSAS is, makes a valuable contribution to the national counterterrorism effort. From the system's introduction in 2002 through mid-2007, the United States never went below yellow alert—elevated risk of terrorist attack—and has gone to orange alert—high risk of terrorist attack—eight times. None of these elevations were terminated by the disruption of a terrorist cell. Only the August 2004 orange alert regarding financial institutions in New York, New Jersey, and Washington, D.C., was publicly associated with subsequent arrests. But even in this instance, there is no evidence that these arrests, involving a terrorist cell in London, resulted from the alert.

Observations Regarding Threat Level Increases from Yellow to Orange, GAO-04-453R (Washington, D.C.: GAO, February 26, 2004), p. 9.

15. See, for example, State of Michigan, "Homeland Security Advisory System," http://www.michigan.gov/homeland/0,1607,7-173—26812—,00.html.

16. GAO, *Homeland Security: Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System,* GAO-04-682 (Washington, D.C.: GAO, June 2004), pp. 12–13, 44. DHS's agency comments on this GAO report did not question its characterization of the HSAS. See also GAO, *Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security,* pp. 39–40.

17. Clinton M. Jenkin, "Risk Perception and Terrorism: Applying the Psychometric Paradigm," *Homeland Security Affairs,* Vol. 2, No. 2 (July 2006), http://hsaj.org/?article=2.2.6; and Scott A. Behunin, "Homeland Security Advisory System," master's thesis, Naval Postgraduate School, 2004.

18. U.S. Northern Command official, phone interview by Jacob Shapiro, April 5, 2006. Northeastern city and state homeland security officials, phone interviews by Jacob Shapiro, March 30 and April 11, 2006, respectively.

19. Cleared threat advisories and information bulletins used to be available at http://www.dhs.gov/dhspublic/display?theme?70 (accessed April 21, 2006), but they were removed in early 2007. All of the cleared advisories deal with changes to the color-coded threat level. Most of the cleared information bulletins are very general.

20. Indeed, the information contained in DHS threat advisories often reaches state homeland security officials through multiple paths at the same time. Susan Reinertson, former homeland security adviser for North Dakota, phone interview by Jacob Shapiro, March 30, 2006.

EARLY DEVELOPMENT

Many observers assume that the HSAS was developed ad hoc, put together in a slapdash manner under severe political pressure and time constraints.[21] Our research suggests that HSAS was not rushed to deployment and that the process was largely a thoughtful attempt to construct a graduated alert system whose terms would be clearly understood by its many users.[22] As guidance for the development of the HSAS, OHS drew on a number of sources, including the U.S. military's Defense Condition system and the Department of Defense and Department of State terrorism warning systems. These latter two involve general threat advisories to which senior local authorities can respond with measures they believe appropriate, a system similar to the private side of the HSAS (i.e., the government-only threat advisories and information bulletins). Initial news coverage of the HSAS announcement also indicated that the system was developed in consultation with police chiefs and state and local governments.[23]

Wherever the inspiration for HSAS was derived, the system was conceived in the chaotic aftermath of September 11. In the month following the attacks, the government issued a series of broad warnings to an anxious public about the possibility of more attacks. During a December 2001 press conference, Homeland Security Director Ridge announced that the government would react to widespread public dissatisfaction with the generality of these warnings by developing a system to standardize public terrorism alerts.[24]

The initial idea for developing the system was that OHS would provide a general framework—the five alert levels—and then agencies and local officials would have twelve months to offer feedback as to what measures they would take at each alert level; in this way, the users of the system were to set protocols.[25] With those protocols in hand, the Homeland Security Council—composed of the president; the vice president; the secretaries of defense, health and human services, transportation, and treasury; the directors of the Federal Bureau of Investigation, the Central Intelligence Agency, and the then Office of Homeland Security; and the assistant to the president for homeland security—would then tailor alert levels to elicit the specific actions it felt were necessary, perhaps even issuing regional, instead of national, alerts. The system's authors

---

21. Lee Herring, "How Would Sociologists Design a Homeland Security Alert System?" *ASA Footnotes,* April 2003.
22. Federal government official, phone interview by Jacob Shapiro, March 10, 2005.
23. Philip Shenon, "Color-Coded System Created to Rate Threat of Terrorism," *New York Times,* March 13, 2002.
24. Ann McFeatters, "Ridge Plans Ranking System for Alerts," *Pittsburgh Post-Gazette,* December 19, 2001.
25. The following is based on a phone interview by Jacob Shapiro with a government official involved in the development of the HSAS while assigned to OHS, March 10, 2005.

believed that these actions would be carried out because the agencies involved would simply be following the protocols they themselves had created. The system as originally conceived presumes an extremely high level of trust in federal authorities and confidence in the value of the information provided, but it does not involve a mechanism for developing and sustaining that trust and confidence. Almost immediately, the system ran into problems, as agencies and localities were diverted to more pressing concerns and never developed the desired protocols, presumably thinking that others would provide sufficient inputs or that OHS itself would develop acceptable protocols.

Following Ridge's March 12 unveiling of the HSAS, the general public and the private sector were asked to comment on the new system. Few of the comments were positive. The American Psychological Association highlighted the ambiguity in the descriptions of the risks at each level, noting that people interpret "low," "high," and "severe" differently. It further noted that the system's conflation of probability and consequence was problematic and suggested separating the two such that yellow might be a "low probability of a high-severity event."[26] The Partnership for Public Warning, a nonpartisan advocacy group, also noted that "HSAS'[s] intentional mixing of risk and probability . . . causes confusion both for the people deciding on the threat level and for those responding to the threat level."[27] Slightly different concerns were addressed in the U.S. Conference of Mayors' comments, which noted that the system did not satisfy local officials' needs for "accurate and timely information which addresses the needs of public safety without creating unneeded public alarm."[28]

HINTS OF POLITICAL MANIPULATION

With the United States on the brink of war with Iraq in February 2003, the George W. Bush administration chose to reduce the threat level from orange to yellow so that it could raise the threat level once the war began. The decision was intended to avoid having to go to red alert. "We don't want to be in a situation where we have to go to red alert, which involves shutting down public facilities and could create a real panic," one anonymous administration official told the press.[29] This was the first publicized case of non-threat-related gerrymandering of the system and further served to erode the system's credibility.

---

26. American Psychological Association, *APA Comment on Homeland Security Advisory System*, April 26, 2002, http://www.apa.org/ppo/issues/shomesecure.html.
27. Partnership for Public Warning, "Comments to the Director of the FBI," April 25, 2002, http://www.ppw.us/ppw/docs/ppw_response.pdf.
28. U.S. Conference of Mayors, "Comments to the U.S. Department of Justice on the Administration of the New Homeland Security Advisory System (HSAS)," April 26, 2002.
29. Quoted in Philip Shenon and Eric Lichtblau, "U.S. Lowers Warning Level to 'Yellow' but Cautions That Serious Threat Remains," *New York Times*, February 28, 2003.

Public opinion polling in 2003 indicated that although the vast majority of respondents could correctly identify the current alert level (73 percent in March 2003), only a slim majority (57 percent) felt the system provided useful information, and only 9 percent reported making any changes to their daily routines in response to the alerts.[30] Rural communities in particular—where there is no obvious terrorist threat—found the nationwide alerts to be both confusing and expensive.[31] Interestingly, partial reimbursements for alert-related expenses are provided only to municipalities that receive grants under the Urban Area Security Initiative, a plan focused on the fifty most threatened urban areas, and to grantees under the Law Enforcement Terrorism Prevention Program.[32] The lack of funding, combined with decreasing trust in the system and declining confidence in the information it provided, led to a steady decline in the responsiveness of local officials to national alerts.[33]

Reacting to concerns about HSAS's credibility, Secretary Ridge announced on June 5, 2003, that DHS would attempt to create a procedure for focused local and regional alerts, as opposed to issuing broad nationwide terrorist alerts. While this was in keeping with the original design of the system, it represented a departure from how the system had been publicly discussed. In September 2003, following strong criticism in a Congressional Research Service report, DHS set stricter internal guidelines for the threat levels.[34] The alert level, DHS decided, would be increased only if there was "credible, detailed evidence of an imminent attack on American soil."[35] Ridge claimed that the basis for the decision was that the nation was now safer from attack, and

30. iPOLL Databank, "Survey by Harvard School of Public Health, Project on Biological Security and the Public and ICR—International Communications Research, March 21–March 25, 2003"; "Survey by Pew Internet & American Life Project, Federal Computer Week, and Princeton Survey Research Associates, August 5–August 11, 2003"; and "Survey by Fox News and Opinion Dynamics, January 7–January 8, 2004," http://www.ropercenter.uconn.edu/ipoll.html.

31. Philip Shenon, "Report Finds Threat Alerts in Color Code Baffle Public," *New York Times,* August 10, 2003.

32. Frances L. Edwards, San Jose emergency manager, interview by Jacob Shapiro, San Jose, California, March 2, 2005.

33. There is ample anecdotal evidence for this decline in confidence in the system. For example, the police department in Phoenix, Arizona, responded aggressively to the first orange alert on September 10, 2002, putting its officers on twelve-hour shifts. Subsequent alerts did not generate such unusual levels of security. See Kevin Johnson, "In Orange Terror Alerts, Wary Cities Hold Back," *USA Today,* July 2, 2003. Utah state officials followed a similar path, raising their state alert level for the first orange alert, but keeping it at yellow for subsequent alerts because of the lack of specific information. See Behunin, "Homeland Security Advisory System," pp. 15–20. A similar pattern of increasing skepticism and decreasing activity in response to alerts emerged during interviews with local officials observing the TOPOFF 3 exercise, held April 5–6, 2005.

34. Shawn Reese, *Homeland Security Advisory System: Possible Issues for Congressional Oversight,* CRS Report for Congress (Washington, D.C.: Library of Congress, August 6, 2003), Order Code RL 32023.

35. Philip Shenon, "High Alerts for Terror Get Harder to Impose," *New York Times,* September 13, 2003.

thus the threshold to move from yellow to orange was higher in 2003 than it had been the year prior. His argument makes little sense in the context of HSAS, which refers only to "significant" or "severe" risks, adjectives that do not depend on some objective baseline level of risk. The sixth orange alert, issued on August 1, 2004, was limited to "the financial services sector in New York City, Northern New Jersey, and Washington, D.C.," reflecting this new approach.[36]

The effects of distrust

Despite these changes, in the lead-up to the 2004 presidential election, the system came under increasing criticism that it was being used as a political tool. On the same day as the sixth orange alert, then presidential candidate Howard Dean stated on CNN: "I am concerned that every time something happens that's not good for President Bush, he plays this trump card, which is terrorism. His whole campaign is based on the notion that 'I can keep you safe; therefore, in times of difficulty for America, stick with me,' and then out comes Tom Ridge. It's just impossible to know how much of this is real and how much of this is politics, and I suspect there's some of both in it."[37] By this time 40 percent of the U.S. public agreed with Dean, believing that increases in the terror alert level were either fully or partially politically motivated.[38]

Scholars have shown that alerts can be politically useful, and research demonstrates a positive, statistically significant increase in presidential approval ratings following warnings about terrorism. President Bush's job approval ratings in the weekly Gallop poll jumped an average of 3 percent following increases in the HSAS's threat level. Major terror warnings, including ones that did not involve increases in the HSAS, produced a statistically significant 2.75 percent increase in President Bush's job approval, even after controlling for the state of the economy and other events that typically affect presidential approval ratings.[39] The effect was not limited to overall presidential approval ratings; approval of the president's handling of the economy also increased following terror alerts.[40] Shortly before the July 2005 orange alert following the

36. Thomas Ridge, "Remarks Regarding Recent Threat Reports," U.S. Department of Homeland Security, Office of the Press Secretary, August 1, 2004.
37. Charlie Savage and Bryan Bender, "U.S. Cites Terror Threats to Financial Facilities, Ridge Raises Alert Level for Washington, NYC, Newark," *Boston Globe,* August 2, 2005.
38. iPOLL Databank, "Survey by Fox News and Opinion Dynamics, August 3–August 4, 2004," http://www.ropercenter.uconn.edu/ipoll.html.
39. Robb Willer, "The Effects of Government-Issued Terror Warnings on Presidential Approval Ratings," *Current Research in Social Psychology,* Vol. 10, No. 1 (September 2004), pp. 1–12, http://www.uiowa.edu/~grpproc/.
40. For the political psychology behind this phenomenon, see Rose McDermott and Philip G. Zimbardo, "The Psychological Consequences of Terrorist Alerts," in Bruce Bongar, Lisa M. Brown,

July 7 London bombings, former Secretary Ridge tacitly confirmed that political pressure had influenced decisions about alerts. Discussing DHS's role in raising the alert level, he stated, "There were times when some people were really aggressive about raising it, and we said, 'For that?'"[41] Given the criticism Ridge has received for his use of the alert system, it is hard to interpret this quotation favorably without assuming that the secretary of DHS lacked access to the intelligence that led other officials to want to raise the alert level.

THE FAILURE OF THE HSAS

Increasing distrust of the alert system led to its gradual disappearance from state and local homeland security planning. There is only one passing reference to the HSAS in the 2004–05 New Jersey Domestic Security Preparedness Task Force Progress Report, a striking change for a state whose leaders had once threatened to close its borders if a red alert were issued.[42] DHS's efforts to salvage the system did little to alter the Gilmore Commission's assessment that "the Homeland Security Advisory System has become largely marginalized."[43]

Such external criticisms led to congressional efforts to change the HSAS. Statutory restrictions on the system were included in the failed Department of Homeland Security Authorization Act for fiscal year 2006. That bill stipulated that "the Under Secretary, under the system, shall not, in issuing any advisory or alert, use color designations as the exclusive means of specifying the homeland security threat conditions that are the subject of the advisory or alert."[44] Similar provisions appear in the fiscal year 2007 DHS authorization bill, which proposes a color-free alert system that would allow for regional and sector-specific targets.[45]

The orange alert issued after the July 2005 London bombings was restricted to the U.S. transportation sector, reflecting a more focused approach to the system. But the alert was issued even when, in DHS Secretary Michael Chertoff's own words, there was "no specific, credible information suggesting an imminent attack here in the United States."[46] The alert level was lowered one month

---

Larry E. Beutler, James N. Breckenridge, and Zimbardo, eds., *The Psychology of Terrorism* (New York: Oxford University Press, 2006), pp. 818–851.

41. Quoted in Mimi Hall, "Ridge Reveals Clashes on Alerts," *USA Today,* May 10, 2005.

42. New Jersey Domestic Security Preparedness Task Force, *2004/2005 Progress Report* (State of New Jersey, 2006), April 20, 2006, http://www.state.nj.us/lps/dsptf/NJDSPTF-04-05-021706.pdf.

43. Gilmore Commission, "Forging America's New Normalcy," p. 27.

44. U.S. House of Representatives, *Department of Homeland Security Authorization Act for Fiscal Year 2006,* H.R.1817.RFS, sec. 223.

45. Tim Starks, "House Panel Considers Security Improvements, Including New Warning System," *Congressional Quarterly Today,* March 28, 2006.

46. Michael Chertoff, "Transcript from Secretary Michael Chertoff Press Briefing on the London Bombings," July 7, 2005.

later because of a lack of specific threats.[47] This use of the HSAS further degraded trust in its usefulness. Raising the alert level without specific information violated the supposedly strict internal standards DHS set in the fall of 2003, sending the message that DHS cannot even be trusted to follows its own procedures. Even worse, the alert was raised when there was no credible, specific information, and then was lowered, according to the DHS secretary himself, because there was no credible, specific information. The tacit message was that the system is arbitrary and is not linked to actual threats. Such a system does not serve to increase state and local officials' confidence about the likelihood of an attack, and using it this way clearly does not instill trust in alerts.

By the beginning of 2006, the HSAS, despite the best intentions of its designers, had failed as an alert system. Following the disruption of a terrorist cell in London on August 10, 2006, the HSAS was raised to red for commercial flights from the United Kingdom to the United States. It is not certain whether this use of the HSAS had any impact independent of the specific actions ordered by the Transportation Safety Administration. The press paid scant attention to the change in color, focusing instead on the plot itself and on the new rules implemented for carry-on baggage.[48]

Despite these problems, the HSAS has served a valuable purpose. A review of the development of state and local standard operating procedures (SOPs), federal government response plans, and various institutions' guides for citizens since September 2001 reveals a gradual convergence on a common language. There have also been significant advances in the sophistication and care with which these documents address public warnings. For example, early drafts of the Washington State homeland security plan contained potentially erroneous information about the criteria for intelligence at each level of HSAS. This information was removed by the time the final version was adopted in late 2004. To the extent that the current system has facilitated a dialogue about warnings and provided a common language, it has certainly been beneficial. In the next section, we briefly review other nations' terror alert systems to provide a context for comparison to the U.S. system.

Terrorism Alerts in Other Nations

Other countries have developed national terrorist alert systems or response plans, most of which differ significantly from the HSAS. Australia uses a tiered

47. Michael Chertoff, "Statement by Homeland Security Secretary Michael Chertoff on Lowering the National Threat Level for the Mass Transit Sector," August 12, 2005.
48. From August 10 through August 14, the five major New York City newspapers ran a mere twenty-four stories containing the words "terror" and "alert," compared with thirty-four containing "terror" and "lines." Of the twenty-four, only six mentioned the color-coded alert system.

public alert system, albeit one without color coding. The British system focuses on keeping much of the threat intelligence secret, announcing threats to the public only when there are specific actions members of the public can take to defend themselves. The French and Spanish alert systems involve public announcements of the level of response plan being invoked, with the plans describing predefined actions at each level. The Israeli system is not formalized, relying instead on the news media to make public the warnings transmitted to the security services. Importantly, only the Australian system entails broad public alerts such as those employed in the HSAS. Countries such as Britain, France, and Israel—all of which have more experience with counterterrorism than does the United States—do not use such systems.

Australia's alert system involves a four-level public warning system.[49] Unlike the U.S. system, which defines risk in terms of both probability and severity, Australia's defines risk solely in terms of the probability of an attack.[50] Australian officials have been reticent about changing their alert level in the absence of specific threat intelligence, leaving it unchanged, for example, after the July 2005 London bombings, which triggered a limited orange alert in the United States.[51] Like the U.S. system, the Australian system has drawn public criticism for being overly general and contributing more to public anxiety than to counterterrorism.[52]

The United Kingdom's terrorist alert system is worth exploring in more detail because of Britain's long experience with terrorism. Its system does not include broad public warnings, nor does it involve color coding. Threat levels in the British system are assigned nationwide, to specific regions, and to economic sectors. These levels are communicated to government and law enforcement agencies and private-sector entities with responsibility for critical infrastructure protection, but not to the public. Alerts are kept secret to protect intelligence sources and avoid alerting terrorists that the government is aware of the threat.[53] Britain's alert system is described explicitly by MI5, the country's security service, to be different from the HSAS. On its website's Frequently Asked Questions page, MI5 defends the British system as having a

---

49. GAO, *Homeland Security: Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System,* pp. 46–47.
50. Australian Government, "National Counter-Terrorism Alert Level," http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/AllDocs/F2ED4B7E7B4C028ACA256FBF00816AE9?OpenDocument.
51. "Australia Reviews Terror Alert Level after London Bombings," Agence France-Presse, July 8, 2005.
52. "Experts Call for Overhaul of Terror Alert System," *Sydney Morning Herald,* September 13, 2005; and George Williams, "Balancing National Security and Human Rights: Lessons from Australia," Fulbright Public Lecture, University of Melbourne, Melbourne, Australia, June 21, 2005.
53. GAO, *Homeland Security: Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System,* p. 45.

"different approach" than the U.S. system: "We do not have one single national system to indicate the current general level of threat." Instead, the Joint Terrorism Analysis Center issues classified threat assessments to different governmental sectors so as to reduce the "damage" to the economy. Public announcements of threats are issued only "when required." MI5 cites the government's policy that the public will be warned of an imminent attack only if a "specific threat emerges against which they can take action to protect themselves."[54]

France and Spain have predefined response plans, and the public is made aware of which plan is being put in place. France uses a color-coded system called Plan Vigipirate. Vigipirate is a four-level preestablished security plan, rather than a warning system designed to alert the public and motivate action by constituent governments.[55] The prime minister's office controls the system, which was raised to red following the July 2005 London bombings, triggering protective measures at specific sites, such as an increased gendarmerie presence at train stations.[56] Each level of the alert requires specific security actions, such as replacing garbage bins with plastic bags or instituting extra security checks at government buildings. Similar to France, Spain uses a three-level, tiered (but not color-coded) response plan called the Terrorism Prevention and Protection Plan, the highest level of which requires the increased screening of passengers on public transportation and heightened security around critical infrastructure. Notably, because of the United States' federal system of government, response plans initiated by the national government that require action at the state and local levels cannot be implemented without significant new legislation.

Israel takes a slightly different approach. The Israeli government issues specific alerts to the military and law enforcement agencies. These alerts are sometimes passed on to the news media, which report them so that members of the public are aware of where and when extra vigilance is warranted. In the days before the Passover holiday in 2006, the police raised Israel's alert to its highest level and announced a total of 73 general terrorist warnings, with 13 regarding specific attacks.[57] Israel issued 578 specific terror warnings in 2005, an average

54. "MI5 Frequently Asked Questions: About Threats to National Security," http://www.mi5.gov.uk/textonly/Page367.html.
55. Ludo Block, "Evaluating the Effectiveness of French Counter-Terrorism," *Terrorism Monitor,* Vol. 3, No. 2 (September 2005), pp. 6–8; and French embassy in the United States, "France's Experiences with—and Methods Combating—Terrorism," http://www.ambafrance-us.org/atoz/terrorism.asp.
56. Alan Cowell, "The New Normal: Wary but Resilient," *New York Times,* September 25, 2005.
57. Efrat Weiss, "Passover Terror Warnings Up," *YNET, Yediot Aharonot Online,* April 9, 2006, http://www.ynetnews.com/articles/0,7340,L-3238110,00.html.

of more than 1.5 per day.[58] With so many warnings, precision and specificity are vital to avoid overwhelming the populace with warnings that do not apply to them. The Israeli government's antiterror task force does issue general threat warnings about travel abroad, but these are more akin to U.S. State Department travel advisories than to the HSAS.[59]

Logic and Purposes of Terror Alerts

The logic of a terror alert supposes that government officials receive information, which could range from information gained from monitoring the level of electronic communications between suspected terrorists to more specific intelligence, about an impending attack. In response, officials raise the alert level to achieve one of three purposes: (1) to prevent an attack; (2) to deter, divert, or defer an attack; or (3) to mitigate the consequences of an unpreventable attack.[60] A system optimally designed for prevention would be secretive and facilitate covert actions by law enforcement. Such a system, however, violates the normative principle that the public has a right to know about security threats. It also misses out on functional advantages that accrue to a system such as the HSAS. Public alert systems can help deter the types of pre-attack behavior demonstrated by the September 11 hijackers—presumably "hiding in plain sight" would be more difficult if the public were more vigilant. If trusted, public systems may create sufficient private incentives to generate the type of target hardening that can lead to deterrence. Finally, in the wake of a successful attack, having given a warning may enhance the government's ability to gain public cooperation and achieve public confidence in the validity of the system.[61]

Of course, prevention, deterrence, and mitigation may not be the only purposes for an alert system. Some scholars have identified far more cynical reasons for the HSAS, including (1) serving as a method of protecting government

58. Israel Ministry of Foreign Affairs, "2005 Terrorism Review," http://www.mfa.gov.il/MFA/Terrorism-?Obstacle?to?Peace/Terrorism?and?Islamic?Fundamentalism-/2005?Terrorism?Review.htm.

59. Yossi Melman, "The Task Force Barked a Warning and Israelis Blithely Streamed South," *Haaretz*, October 10, 2004.

60. Notice this context differs from alerts for natural disasters in two key respects. First, hurricanes, tornadoes, and floods are not strategic actors. The probability of a natural event is not affected when an alert is issued. Second, the "intel" is publicly available, and sharing it does not risk reducing the government's ability to collect information on future events.

61. One key difference between terrorism alerts and systems warning of natural disasters is that when a weather alert is issued, the public can witness the warned-of event. Successful terrorism alerts may lead to nonevents, meaning the public learns nothing about the accuracy of the alert system.

officials from blame in the event of another attack, and (2) functioning as a publicity device to keep terrorism politically salient, favoring the incumbent administration.[62] The first of these alternate reasons can be put in less cynical terms. If politicians have warned of an attack, their calls for citizen action during the response are more likely to be obeyed, meaning they may be better able to deal with the attack's consequences. Leaving these political considerations aside, we argue that the underlying logic is that an alert will start a causal chain ending in outcomes that meet one of the three main purposes. We first examine the logic of alerts and then discuss the core purposes in more detail.

The Logic of Red: A Causal Chain

The Homeland Security Council has one of the three purposes in mind when it authorizes an alert. First, the alert must lead to the desired set of actions by the government and the private sector. Second, these actions must have the intended direct effects. Third, these actions must not have counterproductive secondary effects.[63]

In a federal system, the national government cannot order states, localities, and private industry to take protective actions. Rather, an alert system must provide information that raises actors' estimates of the costs of not taking action above the costs of the desired actions. Assessing these costs involves an application of Bayes's rule, albeit an unusual one that depends on beliefs about the government's likelihood of issuing an alert when an attack is imminent, rather than on an objective likelihood function. Let B be the event an alert is issued and let A be the event an attack occurs. Following Bayes's rule, an actor's post-alert beliefs about an attack are

$$\Pr(A|B) = \frac{\Pr(A)\Pr(B|A)}{\Pr(B)}.$$

Put into words, the belief an attack will occur, given an alert, is the prior probability an attack will occur multiplied by the probability the government will issue an alert before an attack, divided by the probability government will issue an alert. If an alert system is trusted, the perceived prior probability an

62. Philip Zimbardo, "The Political Psychology of Terrorist Alarms," February 26, 2003, http://www.apa.org/about/division/terrorism.html.

63. For example, the primary effect of adding water to a lake would be to raise the water level; the secondary effect might be to add just enough weight to burst a dam, causing extensive downstream damage. Example from Robert F. Graboyes, "Secondary Effects Matter," *Equilibria*, Vol. 1 (1996/1997), http://www.rich.frb.org/pubs/equilibria/issue1/logic.html (accessed February 27, 2005; site discontinued).

alert is issued before an attack is higher. Moreover, the perceived prior probability of a false alert is lower, which decreases the denominator because

$$\Pr(B) = \Pr(A)\Pr(B|A) + \Pr(\neg A)\Pr(B|\neg A),$$

where the second term is the perceived probability of a false alert. Simply put, trusted alerts yield post-alert beliefs about the probability an attack will occur.

Notice the inherent tendency for trust in the alert system to degrade over time. Every time an alert is issued and no attack or arrest of terrorist suspects occurs, beliefs about the probability that an alert will be issued when no attack is imminent increase, thereby reducing incentives to take protective action under an alert.[64] This presents a fundamental paradox for any terrorism alert system: successful use of an alert system degrades trust unless officials can credibly publicize their success.[65] But generating such credibility is problematic, as politicians have strong incentives to claim counterterrorism success regardless of the underlying reality. This paradox suggests that an ideal terror alert system should contain mechanisms for fostering confidence that do not depend solely on politicians' claims.

Tightly targeting alerts also increases the probability of an alert triggering protective actions. Let N be the number of targets subject to an alert, and let H be the event that a specific target is hit. Then each actor's post-alert belief about the probability it will be hit is

$$\Pr(\Pr(H|B) = \frac{\Pr(A|B)}{N-1}.$$

This posterior probability itself consists of two components. The numerator reflects the probability that an attack will take place given that an alert has been issued. The denominator shows the number of other targets subject to the alert.[66] Thus an alert system can increase actors' beliefs about the probability of being hit in two ways. It can use trust to increase their assessment of the chance that an attack will occur, thereby increasing the numerator. Alternatively, making alerts more specific lowers N, thereby increasing actors' beliefs that they will be a target if an attack occurs. Either way, an alert must increase

64. For an intelligence-oriented discussion of this and other concerns, see Freedman, "The Politics of Warning."
65. This paradox is also identified in Bruce Schneier, "Do Terror Alerts Work?" *Rake*, October 2004. It is discussed with respect to warnings about low-probability natural disasters in Michael H. Glantz, "Usable Science 8: Early Warning Systems: Do's and Don'ts," report of "Early Warning Systems" workshop, Shanghai, China, October 20–23, 2003.
66. More generally, the denominator is some nondecreasing function of N.

the actor's posterior beliefs to the point that the costs of protective measures are believed to be less than the private costs of an attack weighted by the posterior probability of being hit.

Generating these necessary beliefs through trust is better than providing specific threat information for two reasons. First, sharing specific information may compromise sources and methods of intelligence. Second, if done publicly, such an information-sharing strategy may reduce the posterior beliefs of those who do not receive additional information. The logic is that when these actors do not receive information, they become more certain they will not be targeted. This in turn lowers the likelihood that they will take protective action. Although terrorists are not infinitely adaptable, they often shift to unprotected targets in the face of site-specific protection. This ability makes information sharing quite problematic. With this in mind, we turn to the three purposes of alerts in light of the logic discussed above.

PREVENTION

The first purpose of an alert is prevention. Going on alert can help prevent future attacks. To do so, the alert must trigger sufficiently heightened attention to lead to the capture of key members of the attack team or, at the very least, produce information that can prevent the planned attack.

The case where an alert is intended to trigger vigilance by law enforcement officials highlights the trust problems inherent in the HSAS. Consider the case of a nationwide alert. For any one official, the probability of encountering a particular suspect will be low. Additionally, the official's belief that an attack will occur in her jurisdiction given that an alert has been issued will also be low because of the overgenerality of HSAS and its lack of credibility. Such an alert thus provides little incentive for an official besieged by higher probability concerns to focus additional attention on counterterrorism. We are not suggesting that officials will never attend to counterterrorism. Rather, the current alert system does not raise posterior beliefs enough to trigger meaningfully increased attention.[67] HSAS did generate increased beliefs when it was first in-

67. The arrest of "millennium bomber" Ahmed Ressam as he tried to enter the United States in December 1999 is entirely consistent with our analysis. First, contrary to much reporting on the incident, no evidence emerged at trial or in interviews with the arresting customs agents to suggest that they knew of any security alert. If an alert had been issued, it must have been issued through sufficiently secure channels that it was not entered into evidence at Ressam's trial. Suppose, for argument's sake, that this is what happened. The fact that a secret alert passed through official channels would motivate increased vigilance does not suggest that a general alert issued through public statements would have a similar galvanizing effect. See Mike Carter, "Clarke Book Has Errors about Arrest of Ahmed Ressam," *Seattle Times*, April 12, 2004.

troduced and was trusted, but the steady erosion of trust meant that by late 2004 law enforcement all but ignored the system.[68]

A similar trust problem applies to the public. In the case of low-probability, high-consequence events, public awareness can play a vital role. For example, Israeli citizens' vigilance toward unusual behavior in public has prevented a number of suicide bombers from achieving their objectives.[69] In a society where incidents do not occur with the frequency faced in Israel, and where there exists a strong culture of protecting personal privacy, generating such attention is a much greater challenge. As in the case of the official above, the incentives for any member of the public to be vigilant are low.[70] As such, an alert must generate a significant increase in public expectations about the probability of an attack if it is to produce the kind of widespread awareness that can make a difference. HSAS has failed in this role.

DETERRENCE

Short of prevention, the second purpose an alert can serve is to deter, divert, or defer a planned attack. The heightened security associated with an alert might deter an attack by sufficiently lowering the terrorists' belief in their chance of success. Such a deterrent effect may not prevent the attack, however; it may simply divert the cell to a new target or cause it to defer the attack to a later date. For example, the cell responsible for the October 2002 Bali bombings initially targeted the U.S. embassy in Jakarta.[71] When surveillance revealed this target was well protected, the attackers shifted to softer targets. A similar dynamic occurred in the shift from hijacking to kidnapping as the modal type of terrorist attack following the installation of metal detectors in airports in the mid-1970s.[72] This is not to say that diverting attacks is not valuable in and of it-

---

68. Because alerts are rarely accompanied by specific intelligence, local authorities are likely to ignore HSAS in favor of actions based on the intelligence they are permitted to see. Behunin, "Homeland Security Advisory System," pp. 21–24. A related problem is that many local officials do not have access to the private "threat alerts" that accompany changes in the alert level. Northeastern city homeland security official, phone interview by Shapiro.

69. Margot Dudkevitch, "Bus Driver Foils Suicide Bombing," *Jerusalem Post*, February 7, 2002; and Margot Dudkevitch, "Bus Driver Prevents Suicide Bombing," *Jerusalem Post*, February 20, 2002.

70. The related psychological problem of the diffusion of personal responsibility is detailed in the work of John M. Darley and B. Latane. See, for example, Darley and Latane, "Bystander Intervention in Emergencies: Diffusion of Responsibility," *Journal of Personal Social Psychology*, Vol. 8 (1968), pp. 377–383. The authors thank Rose McDermott for pointing this out.

71. Wayne Turnbull, "A Tangled Web of Southeast Asian Islamic Terrorism: The Jemaah Islamiyah Terrorist Network," master's thesis, Monterey Institute of International Studies, 2003.

72. Walter Enders and Todd Sandler, "What Do We Know About the Substitution Effect in Transnational Terrorism?" in Andrew Silke, ed., *Research on Terrorism: Trends, Achievements, and Failures* (London: Frank Cass, 2004).

self; shifting an attack on critical infrastructure to a less consequential target would certainly be a powerful, and desirable, effect.[73] So too is delaying an attack, which would give law enforcement more time to track the cell and a better chance of disrupting it.

Here HSAS runs into problems due to the sheer number of targets. Any particular piece of critical infrastructure is unlikely to be targeted. Because the adversary can shift targets, deterrent success requires hardening all easily available sites, not just the ones initially believed to be targets. We expect a kind of "tipping phenomena" with respect to deterrent preventions. Once a critical mass of similar targets has implemented protections, not protecting a target would make it substantially more likely to be hit. Thus an alert system must convince some threshold number of those responsible for critical infrastructure protection in a given area that the chances of an attack are extremely high. The more that alerts influence posterior beliefs, the greater the system's chances of reaching this threshold; and, as stated above, more specific alerts have a greater influence on these beliefs. Failing this, individual incentives will be to skimp on protection.[74] For diversion to have a positive effect on law enforcement's chances of breaking up a plot before an attack, it must not be too easy to find a new, similar target. Generating additional protection over a reasonably wide area, or across similar targets, is essential.

MITIGATION

The third purpose an alert can serve is to mitigate the consequences of an attack by ensuring that emergency operations centers (EOCs) are activated, that communications circuits have been tested, and that first responders are fully staffed and ready the instant an attack occurs.

Maximizing the government's ability to manage consequences of natural disasters is a key goal of many public warning systems, and appears to have been central in the thinking about the design of the HSAS. Half of the mea-

73. For analysis of how governments should take terrorists' ability to shift targets into account when making resource-allocation decisions for homeland security, see Robert Powell, "Defending against Terrorist Attacks with Limited Resources," *American Political Science Review,* Vol. 101, No. 3 (August 2007), pp. 527–541. For an analysis of how this same capability should influence government decisionmaking about sharing sensitive homeland security information, see Jacob N. Shapiro and David A. Siegel, "Is This Paper Dangerous? Balancing Secrecy and Openness in Counterterrorism," Stanford University and Florida State University, 2007.

74. This is exactly the problem noted on the individual level in Scott D. Sagan, "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Lead to Less Nuclear Security," *Risk Analysis,* Vol. 24, No. 4 (November 2004), pp. 935–946. For a discussion of this problem in the context of privately owned critical infrastructure, see Congressional Budget Office, *Homeland Security and the Private Sector* (Washington, D.C.: Congressional Budget Office, December 2004), pp. 2–4.

sures mentioned for orange or red alert in HSPD-3 deal with issues of mitigation. But here the constraints of federalism become problematic. Increasing the staff at EOCs, paying overtime, and prepositioning supplies are all costly actions. Given that the vast majority of response capabilities are in state and local hands, successful mitigation through the alert system requires voluntary, costly compliance. Once again, the lack of trust in and overgenerality of the HSAS mean it no longer generates the beliefs necessary to support such compliance. Moreover, mitigating the consequences from some scenarios may require citizens to take counterintuitive actions. For example, following a nuclear attack, the best option for some survivors would be to shelter in place because the radiation exposure from walking through the fallout would be greater than what they would receive if they waited for radioactive decay to render the fallout less radioactive.[75] A pre-attack alert may increase the likelihood people will follow such recommendations.

Weaknesses of the HSAS

We argue that there are three major weaknesses in the HSAS: (1) contradictions and tensions inherent in the system reduce its credibility and can lead to unexpected actions by both government and private-sector participants; (2) HSAS is extremely sensitive to wrong assumptions about how agents in the system will react because it does not contain defined actions; and (3) the complexity of the system can lead to unexpected, and impossible to predict, secondary effects. The first problem is not inherent in an alert system; rather, it is a result of the specific construction of the HSAS. The final two problems will plague any counterterror alert system, but are exacerbated by the overly general nature of the current system. The key question to keep in mind with these last two problems is whether a different system could ameliorate their impact. We argue that the answer is yes. Taken together, these three problems have significantly diminished the value of the HSAS and have contributed greatly to its irrelevance.

CONTRADICTIONS CAUSING CONFUSION

Alerts under the HSAS were rife with contradictions because (1) it was treated—perhaps incorrectly—as both a pre- and post-attack system both in

75. Ashton B. Carter, Michael May, and William J. Perry, "The Day After: Action in the 24 Hours Following a Nuclear Blast in an American City," report based on April 19, 2007, workshop in Washington, D.C., hosted by the Preventive Defense Project, Harvard and Stanford Universities, May 31, 2007.

policy documents and in national homeland security exercises;[76] (2) by statute it applies only to federal agencies, but it has been treated as a system to which state and local authorities are expected to respond;[77] (3) it was officially intended to trigger government actions, but it has also been used as a public warning system;[78] and (4) it was discussed as both an emergency warning system and a threat advisory system.[79] Exemplifying these problems, DHS's after-action review of the two largest national homeland security exercises to date—Top Officials Exercise Two (TOPOFF 2) in May 2003 and Top Officials Exercise Three (TOPOFF 3) in April 2005—report that in both exercises there was great "uncertainty among participants regarding specific protective actions to be taken by specific agencies under [an] HSAS Severe Threat Condition Red."[80] That federal agencies and constituent governments participating in pre-scripted exercises are confused about their actions at the highest alert level, when it would be most important that they take protective action, provides exceptionally strong evidence that the system causes confusion.[81]

The contradiction between emergency warnings and threat advisories is especially damaging to confidence in the system. An emergency warning entails an implicit call for action. A threat advisory merely provides information to help the public make informed decisions. In congressional testimony in March 2004, Kenneth Allen, executive director of Partnership for Public Warning, neatly summarized the problem of using the HSAS simultaneously as a warning system and an advisory system: "When the threat level was raised over the most recent holiday season, the public was advised to conduct business as usual and continue to make their holiday visits and trips. Such a message creates conflict in the minds of the public between the credibility of the threat and the need to take protective actions—if the threat is credible and serious, why are no changes in behavior warranted?"[82] Admittedly, this contradiction arises

76. On using the alert system in a postattack setting, see "Preparing for the Worst," *Online NewsHour,* May 16, 2003, http://www.pbs.org/newshour/bb/terrorism/jan-june03/cities_05-16.html. For policy documents that treat HSAS as a postattack system, see Washington Military Department, *Guidelines for Implementation of the State of Washington Homeland Security Advisory System.*
77. Benigno E. Aguirre, "Homeland Security Warnings: Lessons Learned and Unlearned" (Newark: Disaster Research Center, University of Delaware, 2003).
78. James Jay Carafano, "Alerting the Nation," testimony before the House Subcommittee on National Security, Emerging Threats, and International Threats, Committee on Government Reform, 108th Cong., 2d sess., March 18, 2004.
79. Allen, "The Homeland Security Advisory System."
80. DHS Office of the Inspector General, *A Review of the Top Officials 3 Exercise* (Washington, D.C.: Office of Inspections and Special Reviews, Department of Homeland Security, November, 2005), p. 30.
81. This is especially true, given that two years passed between these two major exercises.
82. Allen, "The Homeland Security Advisory System," p. 10.

from officials' usage of the HSAS, not from the system itself. Because the system lumps warning and advisory functions together, however, it is inherently vulnerable to such contradictory usage and, in turn, vulnerable to charges of political manipulation.

The confusion over the HSAS was not limited to the public. Government agencies report an inability to determine the appropriate protective measures to be taken based on the alert system.[83] In federal government exercises, agencies have expressed uncertainty about what actions to take and about what actions other agencies would take. Although the Homeland Security Act of 2002 assigned primary responsibility for public advisories to officials within the federal government, many local officials have authority to raise and lower local alert levels. It is not clear that the public or industry understands how to distinguish these local alerts from the national HSAS alert level.

Compounding the problem, some localities establish their own alert levels without publishing any guidelines as to how those levels are chosen. On February 27, 2005, the New York State Office of Public Security website listed the state at yellow and New York City at orange. Although the levels of New York's alert system match those of the HSAS, there was a federal orange alert issued at this time. The yellow alert was a local alert, yet there was no guidance as to how this alert level was reached, who ordered it, or what actions should be taken. Moreover, few localities have followed former New Jersey Governor James McGreevey in stating exactly when they would opt out of national alerts, making interpreting alerts even more challenging.[84] The possibility for confusion is a necessary by-product of a system that induces all involved parties to use the same labels for their alert levels, but does not centralize authority over issuing alerts or require that alert levels be synchronized.

WRONG ASSUMPTIONS

Suppose that an alert overcomes the trust problem. The HSAS still does not specify a set of well-defined and rehearsed actions for lower levels of government and private industry. This means that the decision to use the HSAS, or indeed, any alert system, necessarily depends on a set of assumptions about how constituent governments and private entities will react. Thus, whether an alert can meet its intended goals depends on whether those assumptions are correct. Although this is true even for an alert system involving well-rehearsed

83. GAO, *Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security,* p. 40.
84. Mark Rosman, "Agencies Can Make Red Alert Specific to New Jersey Sites," *Tri-Town News,* March 27, 2003.

plans, wrong assumptions are more likely to be problematic in a system such as the HSAS, which contains no mechanism for correcting them.

One type of wrong assumption stands out in disaster response plans: the belief that all things not directly affected by the alert will remain the same as before. Planners have assumed that off-duty doctors will report to work in quarantined zones, that sewage treatment plant workers will show up if their facility is in an affected zone, and that mail carriers will enter a potentially infected zone to deliver prophylactic antibiotics.[85] Even when critical assumptions are shown to be false, they tend to remain embedded in planning documents. Hospital plans for mass casualties rely on sharing resources with nearby facilities—a problem for attacks with widespread consequences—and bio-attack response plans still presume that doctors will show up for their shifts despite strong evidence to the contrary.[86] The current alert system contains no mechanism to identify and to correct such problematic planning assumptions.

The lack of such a mechanism also means that the HSAS is likely to fall victim to mistaken assumptions about the background conditions built into response plans. Historically, the conditions assumed in action plans for low-probability/high-impact events that have not been well rehearsed have not prevailed when those events occurred, and thus the plans have not been followed.[87] For example, during the *Exxon Valdez* oil spill of March 1989, the SOPs that had been established for such an event, such as immediately deploying containment booms and oil skimmers, were not followed. Part of the problem was that those SOPs were designed on the assumption that the spill would only take place in a low sea state where skimmers could function. These are exactly the conditions under which a spill was least likely. So when a spill did occur in a higher sea state, the response was ad hoc, booms and skimmers could not be deployed, other elements of the plan were not implemented, and the spill took years to clean up.[88] Plans are useful analytical devices to be sure, and no one expects perfect implementation. Our concern is that if the decision to go to on-alert status is based on the belief that scenarios embodied in these plans will play out largely as expected, decisionmakers may get something vastly different than what they intended.

Indeed, if state-level response plans submitted during exercises are any indi-

85. Edwards, interview by Shapiro; and Salvatore S. Lanzilotti, "Hawaii Medical Personnel Assessment, 2003" (Honolulu: Hawaii Department of Health, 2004).
86. Union Hospital and St. Barnabus Health Care System officials interviewed by Jacob Shapiro during TOPOFF 3 exercise, Union, New Jersey, April 5–6, 2005.
87. Lee Clarke, *Mission Improbable: Using Fantasy Documents to Tame Disaster* (Chicago: University of Chicago Press, 1999).
88. Lee Clarke, "Oil-Spill Fantasies," *Atlantic Monthly,* November 1990, pp. 65–77.

cation, then much of the target hardening that occurs at the state level in response to federal alert levels may not be what decisionmakers would expect. Two examples stand out from our discussions with officials and analysts observing TOPOFF 2 and TOPOFF 3. One state determined that, in light of the increased rate of foreclosures forced by the economic downturn that would follow a red alert, bankruptcy courts—which might be targeted by angry farmers—should be protected. Another state wanted to protect a rail junction in a remote location, through which 90 percent of the state's cattle traveled because it was a point of high vulnerability for the state's economy. It is difficult to argue that these are the targets that the Homeland Security Council will imagine it is protecting by going on alert. In general, it is not clear that states will react to increased alert levels by protecting what federal authorities assume they will.[89]

systemic complexity

The HSAS is also vulnerable to failure because of its intrinsic complexity. Although complexity may be inherently problematic in any terrorist alert system, we argue that the overly general application of the HSAS exacerbates these problems. There are at least six types of strategic players in the HSAS system: (1) federal government agencies; (2) state government agencies; (3) local government agencies; (4) the media; (5) businesses; (6) private citizens; and (7) the adversary. There may be many players in each type, all reacting strategically to one another. An alert for the New York metropolitan area, for example, would involve the terrorists, at least four federal agencies,[90] four states, thirty-six counties, numerous small cities and municipalities, at least nine local television stations, thousands of firms, and millions of citizens.[91] Some of the interactions between these players can be predicted. Our contention, however, is that the HSAS acts on a complex interactive system.[92] Such a system has three characteristics: (1) there is a diverse set of agents; (2) these agents interact locally over time; and (3) the agents react strategically to each other's actual and expected actions.[93] Taken together, these characteristics mean the system is

89. Aguirre, "Homeland Security Warnings," p. 8.
90. The four are the Federal Emergency Management Agency, the Federal Bureau of Investigation, the Coast Guard, and the Transportation Security Administration.
91. *Ranking Tables for Metropolitan Areas: Population in 2000 and Population Change from 1990 to 2000* (Washington, D.C.: U.S. Census Bureau, 2000).
92. A similar perspective was reached independently in Louise K. Comfort, Mark Dunn, David Johnson, Robert Skertich, and Adam Zagorecki, "Coordination in Complex Systems: Increasing Efficiency in Disaster Mitigation and Response," *International Journal of Emergency Management*, Vol. 2, No. 2 (Spring 2004), pp. 62–80.
93. This definition combines elements from a variety of sources, including Simon A. Levin, "Complex Adaptive Systems: Exploring the Known, the Unknown, and the Unknowable," *Bulletin of the American Mathematical Society*, Vol. 40 (October 2002), pp. 3–19; and Kevin Dooley, "Complex

likely to exhibit novel, emergent behavior that may fit a general pattern but that cannot be deterministically predicted.

The system made up of the actors responding to an HSAS alert fits this definition. Thus, accurate prediction of the system's response is, simply put, inherently impossible.[94] So even if each agent reacts to the alert as expected, and even if all underlying assumptions are correct, unexpected interactions may occur as the players in the system react to one another's initial actions, resulting in outcomes that will almost surely be different than what is predicted. Given these facts, it is reasonable to ask how any system can do better. By focusing on three of the mechanisms that create unexpected interactions, we can identify characteristics of the current HSAS that exacerbate this problem.

First, highly general public alert systems such as the HSAS are especially likely to have counterproductive effects because they trigger reactions by so many actors. Under some bio-attack scenarios, for example, an alert may hinder vital early detection efforts as a concerned public flocks to emergency rooms demanding to be tested and given drugs. Just such a public response occurred in several areas during the October 2001 anthrax attacks.[95] Moreover, some emerging detection technologies for biological attacks rely on purchasing patterns for over-the-counter analgesics.[96] An alert that increased the salience of personal health would likely skew these patterns, reducing the value of the detection system.

Second, protective measures are more likely to create unexpected consequences in a system such as the HSAS where there is no established, extensively researched set of protective measures upon which officials can draw. One example of the kind of unexpected consequences of particular concern is the side effects of increased inspections along the U.S.-Mexican border that were phased in throughout the 1990s. These inspections have resulted in such delays that shippers do not want to pay reliable, modern trucks to sit and run the gauntlet of inspections. Many shippers now offload full shipments, put them onto cheaper trucks run by questionable companies, get the shipments through the time-consuming customs process, and then reload on the other side with a reliable commercial shipper. The result, aside from significant inef-

---

Adaptive Systems: A Nominal Definition," October 26, 1996, http://www.eas.asu.edu/?kdooley/casopdef.html.

94. W. Brian Arthur, "Complexity and the Economy," *Science,* Vol. 284, No. 5411 (April 1999), pp. 107–109.

95. GAO, *Public Health Response to Anthrax Incidents of 2001,* Report 04-152 (Washington, D.C.: GAO), pp. 17–18; Neely Tucker and Carol D. Leonnig, "For SW Area, Anthrax Discovery Arouses Anxiety," *Washington Post,* October 27, 2001; and Leef Smith and Avram Goldstein, "Jittery Patients Pack Hospitals," *Washington Post,* October 26, 2001.

96. Doug Frisdma, Center for Biomedical Informatics, University of Pittsburgh, private communication with Jacob Shapiro, June 22, 2004.

ficiencies, has been a windfall for the smugglers and organized criminals who run the lucrative short-haul cross-border trade. Preventing this trade is impossible without extensive surveillance to stop any reloading of trucks within fifty miles, or more, from the border. Thus enforcement along the border creates the market conditions that support this vulnerable short-haul trucking sector.[97]

Third, state- or local-level actions may be deeply incompatible. This is especially likely in a system such as the HSAS, which does not contain a formal process for coordinating response plans. Indeed, the DHS inspector general's report on TOPOFF 3 found that in both TOPOFF 2 and TOPOFF 3, "many agencies lacked an understanding of the protective actions that might be taken by other agencies or jurisdictions under various threat levels."[98] Other conflicting plans have been identified only through exercises, highlighting the value of forcing actors involved in the alert system to discuss their plans before an alert is issued. According to one state's emergency manager, a major city had plans to evacuate into a neighboring state in response to a radiological plume created by a dirty bomb. But, the evacuating city had not informed its intended destination, the neighboring state, of this plan. The destination state's plan for an HSAS red alert included closing highways, according to interviews given by a senior official in that state.[99] The necessity of coordinating local responses has been recognized and is identified as a national priority under the draft National Preparedness Goal released in December 2005. Such coordination has not yet occurred, however; and the current alert system offers no incentives for such action.[100]

The problems we highlight in this section were demonstrated in the aftermath of Hurricane Katrina. In the case of Katrina, a national alert of sorts was issued—President Bush's preemptive disaster declaration more than thirty-six hours before Katrina's landfall—to enhance mitigation efforts, but the system of actors responding to the alert hardly behaved as federal officials expected. Three examples illustrate the problem. First, news organizations vastly overexaggerated reports of violence after the storm. These reports in turn slowed the response to the disaster as organizations awaited the reestablishment of law and order. The reports also led one neighboring suburb, Gretna, to prevent thousands of New Orleans residents from evacuating over a bridge connecting the two communities.[101]

---

97. Flynn, *America the Vulnerable,* pp. 65–66.
98. DHS Office of the Inspector General, *A Review of the Top Officials 3 Exercise,* p. 30.
99. Julia Loughran, Thoughtlink, private communication with Jacob Shapiro, July 13, 2004. Thoughtlink provided contractor support for a number of DHS exercises in 2004.
100. Department of Homeland Security, *National Preparedness Goal (Draft),* December 2005. No final version has been issued.
101. Robert E. Pierre and Ann Gerhart, "News of Pandemonium May Have Slowed Aid," *Washington Post,* October 5, 2005.

Second, the response was further slowed by incompatible actions at the state and federal levels. Given advanced warning, all parties prepared as they saw fit. For Louisiana emergency management personnel, this meant focusing all pre-landfall efforts on evacuations. Consequently, Louisiana did not assign staff to work with the Federal Emergency Management Agency to plan initial mitigation efforts for after the storm passed. This failure to coordinate significantly slowed federal assistance in Louisiana relative to Mississippi and Alabama.[102]

Third, the evacuation was hampered by strategic agents acting on incorrect beliefs. Here Jefferson Parish President Aaron Broussard stands out. Broussard believed that he did not have the capacity to enforce a mandatory evacuation order, and so did not issue one.[103] Most other officials understood the use of the term "mandatory" in evacuation orders as an exhortative measure with no legal status, and no other locality worried about its capacity to enforce these orders.[104] The absence of a mandatory evacuation order in Jefferson Parish, New Orleans's neighbor to the southeast, led to much lower rates of evacuation, dramatically worsening search-and-rescue requirements in the storm's aftermath. Thus, the Katrina response shows how a series of reasonable strategic reactions to local conditions led to a host of unexpected difficulties in managing the aftermath of the disaster—a classic example of a complex adaptive system.[105]

Our brief discussion of several of the problems in the Katrina response highlights how in a complex interactive system, such as the one the HSAS is designed for, it is very likely that unexpected interactions will occur, leading to unexpected outcomes. The experience with Katrina suggests the difficulties of designing a system intended to affect so many actors' behavior in the days surrounding a major disaster. Actions taken by different parts of the system may be incompatible in unexpected ways. Protective measures may produce perverse incentives that make the country less secure. Locally rational decisions may create problems with repercussions throughout the system. Taken together, there are strong reasons to believe that a system such as the HSAS will

102. Department of Homeland Security Office of Inspections and Special Reviews, *A Performance Review of FEMA's Disaster Management in Response to Hurricane Katrina* (Washington, D.C.: Office of Inspections and Special Reviews, Department of Homeland Security, March 2006), p. 21.
103. Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina* (Washington, D.C.: Government Printing Office, 2006), pp. 109–111.
104. Ibid., p. 110.
105. Katrina also demonstrates the harsh reality that some disasters are so large that going on alert might not accomplish much.

not deliver what is expected. As we noted, however, the general patterns of a complex interactive system can be identified through repeated observation. In the next section, we suggest an alternative system that ameliorates many of the problems we have identified here by creating incentives for just such repeated observation.

An Alternative System

We have argued that the core challenge for an alert system in the United States is to motivate actors to take costly voluntary action in the absence of federal authority. So why not suggest that the federal government simply pass legislation requiring state and local governments to take certain actions during terrorist alerts? There are three reasons why doing so is undesirable. First, it is not clear that excising state and local governments' discretion in this area is an ideal solution. Federal officials often suggest inappropriate or unrealistic actions, whereas local officials identify more functional responses.[106] Second, there is a long tradition in the United States of emergency and disaster response being the purview of local governments, and efforts to centralize responses to terrorism warnings—and responses to other potential disasters—will inevitably run afoul of constitutional structures that define the United States' federal system.[107] Third, even if Congress wanted to thwart tradition, there are substantial pressures from organized interests that would make such legislation difficult, if not impossible, to pass. Private owners of prospective targets where the social costs of an attack greatly outweigh the private costs have both a strong interest in minimizing spending on protection and a proven record of effectively opposing compulsory protective measures.[108]

---

106. Edwards, interview by Shapiro; Susan Reinertson, phone interview by Shapiro; and Northeastern state homeland security official, interview by Shapiro, April 11, 2006. Federal action plans have been circulated that contain improbable and empirically contradicted assumptions about how first responders will behave in the wake of an attack. See, for example, Lanzilotti, "Hawaii Medical Personnel Assessment, 2003."

107. Herman B. Leonard, "Katrina as Prelude: Preparing for and Responding to Future Katrina-Class Disturbances in the United States," testimony before the U.S. Senate Homeland Security and Governmental Affairs Committee, 109th Cong., 2d sess., March 8, 2006, pp. 5, 6, 10.

108. Chemical industry associations have even argued that more stringent state laws should be superseded by any new federal legislation, effectively seeking to implement the minimum feasible level of protection. See Dana A. Shea, *Legislative Approaches to Chemical Facility Security,* CRS Report for Congress (Washington, D.C.: Library of Congress, April 12, 2006), Order Code RL 33043, p. 21. On incentives to minimize security expenditures, see Congressional Budget Office, *Homeland Security and the Private Sector;* and Carl Pine, "EPA's Security Push Fails," *Pittsburgh Tribune-Review,* July 14, 2002. For examples of the impact of chemical industry lobbying, see John Mintz, "Bush Seeks Voluntary Chemical Plant Security Steps," *Washington Post,* April 8, 2003; Frank J. Cilluffo, testimony before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Homeland Security Committee, 109th Cong., 1st sess., June 15, 2005; and Bob

Given that legislative action to provide the federal government with statutory authority under an alert is unlikely, and may well be undesirable, we now turn to a discussion of an alternative alert system, beginning with a brief summary of four major problems with the current version of the HSAS. First, all alert systems are subject to a paradox: if the alert "works," or prevents a terrorist attack, the system has a diminished impact on beliefs the next time one is used. Second, contradictions and confusion inherent in the HSAS further reduce trust in the system and make it less likely that the desired actions will be taken. Third, wrong assumptions are particularly likely when there is no defined action to take and no rehearsals of what these actions might actually involve. Finally, systemic complexity proves especially detrimental when the system is so broad and there are no mechanisms to force those affected by the system to identify incompatible plans and incorrect beliefs.

Because achieving compliance from actors through trust is better than the alternative option—achieving compliance through information sharing—we suggest a system that maximizes trust without revealing potentially damaging information. Developing trust in a terror alert system is inherently difficult, however, because governments prefer not to share the information behind alerts, even long after alerts have passed. As an alternative, we suggest that governments attempt to generate trust through "procedural fairness."

Procedural fairness refers to the idea that in the absence of information about the trustworthiness of an authority, people react more favorably to—and are more likely to comply with—the authority's actions if the authority is perceived to use a just decisionmaking procedure.[109] An extension of this finding is that voluntary compliance with authority is enhanced when individuals trust an organization's regulations and decisions.[110] This trust, in turn, is greater when people feel that an organization has followed fair procedures.[111] In the alert context, information about trustworthiness is unavailable to anyone who does not have access to the (often) classified materials supporting an alert. As such, if the process by which an alert is issued is understood, and is perceived as being fair, then the probability of voluntary compliance will be

---

Slaughter, testimony before the Senate Homeland Security and Governmental Affairs Committee, 109th Cong., 1st sess., July 13, 2005.

109. Kees van den Bos, Henke A.M. Wilke, and E. Allan Lind, "When Do We Need Procedural Fairness? The Role of Trust in Authority," *Journal of Personality and Social Psychology,* Vol. 75, No. 6 (December 1998), pp. 1449–1458.

110. Tom R. Tyler, *Why People Obey the Law* (New Haven, Conn.: Yale University Press, 1990); and John Braithwaite and Toni Makkai, "Trust and Compliance," *Policing and Society,* Vol. 4, No. 1 (1994), pp. 1–12.

111. E. Allan Lind and Tom R. Tyler, *The Social Psychology of Procedural Justice* (New York: Plenum, 1988).

higher.[112] In the failed HSAS, little information is shared, and the process is neither trusted nor understood.[113]

To develop a sense of procedural fairness, and address the other problems we have identified, we suggest an alternative system in which DHS works with the relevant actors to develop a set of specific actions that are available at each level of the alert. Some of this type of work has been done ad hoc through a variety of programs. Although this has led to a steady increase in the sophistication of alert- and preparedness-related documents over the last three years, it has not been effectively formalized with respect to the alert system. What we propose is substantively different from what DHS has done before. In the past, DHS solicited inputs only from federal and state agencies on what they would do at each alert level. This information was requested without reference to any criteria DHS would use for determining alert levels, and industry was not included in the conversation.[114] As such, the procedure did little to develop a widespread sense of trust in DHS officials or to build confidence in the process DHS would follow for calling an alert.

Instead, we suggest a system where the Homeland Security Council could order a colored alert with supplemental measures *A*, *B*, and *C* for region *X*. The colored alert levels by themselves would entail only those cheap, commonsensical measures—updating phone numbers for colleagues in other government agencies, for example—that are useful in any contingency. These measures are already specified in many states' SOPs. Supplemental measures would consist of highly specific actions, such as requiring escorts of certain types of hazardous materials shipments or doubling the guard force at designated industrial facilities.

As part of the process of negotiating these measures, explicit standards would have to be laid out for what type of intelligence would trigger each set of supplemental measures. Actions that entailed significant economic dislocation would require a higher standard of proof. In such a system, industry and local authorities would have to think through exactly what they are willing to do given certain indicators. The idea would be that if asked to take measure *A*, industries and states would be able to realize implicitly how serious the intelligence was without having to see the actual intelligence. This knowledge, combined with the repeated interactions inherent in the negotiations process,

---

112. Tom R. Tyler and Peter DeGoey, "Trust in Organizational Authorities: The Influence of Motive Attributions on Willingness to Accept Decisions," in Roderick M. Kramer and Tyler, eds., *Trust in Organizations: Frontiers of Theory and Research* (Thousand Oaks, Calif.: Sage, 1996), pp. 331–356.
113. GAO, *Homeland Security Advisory System: Preliminary Observations Regarding Threat Level Increases from Yellow to Orange*, p. 7.
114. U.S. government official, phone interview by Jacob Shapiro, March 10, 2005.

would generate beliefs in the fairness of the government's alert procedures, and hence facilitate a sense of procedural fairness and trust. In traditional political science terms, the negotiation process would enhance the government's reputation with the various players involved in the HSAS and increase the credibility of the government's signals.

This alternative alert system has four advantages. First, it reduces the need for public negotiations over compliance in the midst of a crisis, which can reveal useful information to the terrorists. Observing government officials discussing specific measures over a system such as CEO Comlink—a homeland security information-sharing system created by the Business Roundtable that links 150 chief executive officers with one another and with government officials—is much more difficult than viewing a public news conference calling on local firms to take a specific action. Second, by prenegotiating the actions possible at each level of the alert, our system would dramatically reduce confusion, making it clear to the relevant actors when the system is being used as a warning and when it is being employed as a threat advisory. Third, the prenegotiation process would increase the likelihood that problematic assumptions would be identified under benign conditions, reducing the problem of wrong assumptions. Fourth, the process would also increase the chance that incompatibilities in action plans would be worked out, reducing the problem of systemic complexity. Admittedly, this prenegotiation process would reveal information about government concerns and about the types of intelligence that trigger alerts. The probability of revealing such information would be lessened, however, if the negotiations process were embedded in existing exercise programs. Moreover, the costs of revealing such information would likely be outweighed by the enhanced responsiveness of the alert system.[115]

Although the paradox of an alert system will always be present, our alternative would place countervailing pressures on the tendency to lose trust in the alert system and in the value of the information it provides. Of course, we recognize that given the HSAS's poor reputation, there are significant impediments to instituting a new system, including significant up-front contracting costs to the types of prenegotiations that would be required to effectively implement our system. The original design for the HSAS was similar to our system in that it was supposed to rely on feedback from national agencies and local governments. One reason those protocols were never developed was that constituent governments had to shoulder all the contracting costs but received

115. Jacob Shapiro and David Siegel identify a wide range of conditions under which sharing a government's private information can enhance counterterrorism efforts by supporting more effective prevention and target hardening. Shapiro and Siegel, "Is This Paper Dangerous?"

nothing in return. Participation in the prenegotiations can be motivated by tying them into existing exercise programs and by making participation a condition for receiving DHS preparedness grants. Nevertheless, the negotiations would be costly, and the HSAS's low credibility would make it hard to gain political support for paying these contracting costs.

We therefore suggest a more modest way forward. Reform should start on a small scale by developing our system among the forty-six most threatened urban areas as identified by the Urban Area Security Initiative.[116] Participation in the prenegotiations could be compelled by using administrative rules procedures to make participation a condition for approving initiative grants. As the system begins to generate more confidence, we suggest gradually expanding the playbook of prenegotiated actions to include more state agencies and private entities. The specifics of the actual playbook are far less important, however, than creating both the knowledge that comes out the process and, most important, rebuilding the belief that an alert system can provide valuable information.

This alternative system would solve many of the problems we have highlighted with the HSAS. Compliance would be greater both because prior agreement over the criteria for actions would generate a sense of procedural fairness and because the negotiation process itself would provide opportunities for building trusted relationships. Opportunities for confusion would be reduced because the negotiations process provides a formal venue for resolving misunderstandings between levels of government and between government and industry. Because measures would be prenegotiated, there would be more opportunities to identify key background conditions that would be affected by the alert, such as the percentage of doctors reporting to work following a terrorist attack. Negotiations would also provide a vehicle for learning about how the system affected by the HSAS would likely behave in an emergency, reducing the challenges of systemic complexity.

Conclusion

We have discussed the failure of the Homeland Security Advisory System in the context of the fundamental tasks for an alert system in a federal government. A functional alert system must sufficiently increase beliefs about the value of protection, and it must generate predictable outcomes that match the purposes for an alert. The current alert system in the United States fails at

116. Department of Homeland Security, "Fiscal Year 2006 UASI Eligibility List," http://www.dhs.gov/xlibrary/assets/FY06_UASI_Eligibility_List.pdf.

both tasks. In response to these problems, we have offered an alternative system. Our system would use a prenegotiated playbook of possible actions for each alert level to enhance confidence in the system and would create a process that increases the predictability of the alert system.

No one with whom we spoke in researching this article believes that the HSAS has been effective. Given the failure of the HSAS, the time has come to take on the challenge of creating a better system. The argument set forth in this article lays the groundwork for rethinking the system. Along the way, we have offered insights about the strategic challenges faced by any alert system. Where leaders seek to motivate costly voluntary actions, but not share the private information compelling action, mechanisms for building a sense of procedural fairness and confidence in the value of the information provided are absolutely critical. This insight has strong implications for many public policy problems, but it is critically important for terrorism alert systems.