"The Management Challenge of Extreme Events"

Sally Katzen
Former Senior Government Official
Currently Teaching at Smith College and Johns Hopkins University

There were two professional experiences that I had that influenced my approach to the issues that were raised by the events of September 11th. Both occurred while I was serving as a senior government official in the Clinton Administration.

The first began over a decade ago. As a political appointee in the Executive Office of the President, I was asked to participate in preparing for the unimaginable. That was how it was phrased. For the next eight years, I was deeply immersed in preparedness.

The primary concern was an attempt (or success) of decapitating the federal government. How would successor presidents function in a world that was vastly different from the world as we knew it? Recently, there have been newspaper accounts of continuity of operations plans and the dusting off of "cold war" plans for successor governments. There are also newspaper accounts of civil servants in secret bunkers preparing to do what is necessary to ensure that government continues to function. Most of the information surrounding these matters is classified, and the specific work I undertook and my particular experiences are obviously off-limits. Nonetheless, this assignment gave me an opportunity, well before September 11th, to think about how the public sector thinks about "extreme events."

In the wake of September 11, I found myself watching and analyzing the nation's reaction to the activities of the leadership in Washington. President Bush went to various secure sites in the country before returning to the Capitol. There followed an effort to keep the President and the Vice President from being in close proximity to one another for an extended period of time. These actions spoke volumes. The country was also waiting for the President's first words and then for his "more informed" comments. What was the

reaction to the tone of his speech(es)? The content? There were also issues of how fast and how accurate was the information being sent to the White House, particularly as to the amount of damage sustained from the attacks, the steps being taken to secure the country, and the plans for retaliation. Were the people charged with making decisions operating from the same databases? Same assumptions? Also, at what point should information be shared with the public? How much confirmation of the information is appropriate before it is widely disseminated?   What types of information are likely to be informative, rather than leading to either complacency or panic? And how do you balance the public's right to know and the interests in security? These issues are inevitably affected by a host of factors and one size cannot fit all. My initial take is that there is usually a lot of information, but much of it is often inconsistent and, in any event, inconclusive. While the content of the message from the leaders is very important (and here more information is better than less), the tone is critical. With respect to information and communication issues arising after September 11th, we have all experienced the inadequacy of the "high alert" warnings from the Office of Homeland Security. Recently, Governor Ridge unveiled a "color coded" alert system. But is it really an improvement in enabling Americans to understand the risks and to take actions to mitigate those risks? Also there is currently a stand-off between the Congress and Governor Ridge as to whether he will testify before Congress. There are precedents to support both sides. Are there ways to minimize friction between the branches of government on information issues? And to what extent is his decision not to testify influenced by his reluctance (legitimate or not) to answer under oath some of the questions that may be put to him?

The second professional experience I had is perhaps the closest analogy to the threat of terrorism (or other extreme events) -- Y2K. In the early 90's, I was the person at the Office of Management and Budget (OMB) responsible for information technology policy, and I spent an increasing amount of time on the issue, until I concluded (in 1995-96) that it needed the attention of someone full time   -- someone who would wake up each morning and ask how we are preparing ourselves, what are the vulnerabilities, and what information is useful for the public to respond without panicking (how many people

ultimately stored batteries, water, canned foods, etc.?) I helped recruit John Koskinen as the Y2K czar and agreed to serve as Vice Chair of his Task Force.

OMB continued to be "in charge" of the government's Y2K problems, so I worked with all of the agencies in increasing awareness, sharing best practices, developing contingency plans, and finding the funds to pay for it all. John Koskinen's Task Force picked up the private sector (which was in various stages of preparedness), coordinated with state and local governments, and reached out (through a new United Nations committee) to countries around the globe. Like the threat of terrorism, Y2K was a global phenomenon, the private and public sectors were inextricably linked, and the approach to the public had to be candid, complete but always constructive. Unlike the threat of terrorism, Y2K was a specific problem that was set to occur at a certain time, and after that moment we would know whether we had succeeded or not.

Through this experience, I came to value greatly public-private partnerships. Y2K's success was largely attributable to those partnerships. But to be successful, such arrangements must be based on mutual respect, lack of suspicion, and a sharing of information, whether it reflects well or poorly on the public or private sector. It is also critically important that the lines of responsibility be clearly defined. With Y2K, the government was responsible for the remediation of its computers (properties) and the private sector was responsible for remediation of its computers (properties). For prophylactic measures, that makes eminently good sense. It is not necessarily the formula for recovery from damages; there are circumstances where the government should step in (see below).

The Y2K experience was also informative about the usefulness of risk assessments and cost-benefit analyses. To my mind, they were useful but clearly not dispositive. Moreover, we were dealing with known risks and had a very good handle on the costs of remediation of the problem in most circumstances. The same cannot be said with respect to threat assessments from acts of terrorism. Consider the various steps taken

immediately after September 11 to heighten security on the airlines. Much of the effort went to avoiding bombs on planes (e.g., bag matching, no curb-side check-in), not hijackers prepared to take their own lives. The various ways of inflicting enormous damage are almost boundless, and the choice would be deliberate (rather than nature taking its course in a random but discernible pattern , e.g., hurricanes, floods, etc.). which makes the traditional risk assessment and cost benefit analyses considerably more difficult and less useful. (I say this even though I spent five years at OMB encouraging agencies to improve their cost-benefit analyses and risk assessments).

Finally, my experience at OMB has made me acutely aware of the many demands for the federal government to foot the bill for anything out of the ordinary. Good arguments can always be advanced for why the individual or group affected should not be expected to bear the costs of recovering from a particular catastrophe. However persuasive these arguments may be, there are only limited resources (even though we are back in deficit spending), and paying for recovery for one group generally means less is available for another pressing need. Also, the government is not as efficient or effective as private markets in various areas (e.g., reinsurance). Nonetheless, the equities are usually fairly clear and often persuasive, if not compelling. The government can and should, I believe, step in when those affected are not to blame and the burden is too great for them to finance their recovery, although it may well be appropriate to impose conditions on the recipients to assist in mitigation.