Homeland Security and Consequence Management

Richard Falkenrath
Visiting Fellow, Foreign Policy Studies
The Brookings Institution

Day IV

Of all topics related to the war on terror, the proliferation of weapons of mass destruction, and homeland security, "consequence management" is surely the most dismal, for it has as its antecedent the failure of the highest priority objective in this area, prevention. When policy makers are called upon to manage the consequences of a terrorist attack, their efforts to prevent the attack have failed. Moreover, the term "consequence management" is too narrow to capture properly all the steps that the U.S. government would take in response to a terrorist attack, a credible terrorist threat, or another such incident of national significance. Hence, this paper will use instead the term "incident management."

The U.S. government has initiated major changes in its incident management system in the three years since the 9/11 attacks. This new system is, in many respects, a work in progress. Many of the changes currently underway are not well understood outside the government or even, in some cases, within the government. This paper will describe the emerging new national incident management system – principally from a point of view at the apex of the system, the White House.

The paper will provide a few comments on how incidents of national significance are managed in general. It will then offer a number of observations about the special challenges presented by the two most extreme WMD threats: nuclear weapons and biological weapons, and conclude by summarizing a number of outstanding policy challenges in the area of incident management.

The single most significant reason why incident management is important is that lives can hang in the balance. Effective incident management is also critical to maintaining the public's confidence in the government during crises or times of stress. Unfortunately, it is all too easy for senior officials to relegate incident management to low-level specialists, who labor away in obscurity only to find their plans and procedures swept away at a moment's notice by the press of events or the idiosyncrasies of principals whom they do not know.

Federal Roles and Responsibilities

Federal roles and responsibilities have changed significantly over the three years since 9/11. Before then, national policy was set by Presidential Decision Directive 39, which divided operational responsibilities between the FBI, which handled "crisis management," and FEMA, which handled "consequence management." Other federal departments and agencies would provide

support to one or the other of these agencies. Overall coordination was performed by the National Security Council staff.

President Bush ordered changes in this basic structure almost immediately after 9/11, starting with Executive Order 13228, which established the Office of Homeland Security (now called the Homeland Security Council) in the White House Office and directed that the "Assistant to the President for Homeland Security shall be the individual primarily responsible for coordinating the domestic response efforts of all departments and agencies in the event of an imminent terrorist threat and during and in the immediate aftermath of a terrorist attack within the United States and shall be the principal point of contact for and to the President with respect to coordination of such efforts."

At the same time, President Bush signed National Security Presidential Directive-8 (NSPD-8), which established the position of Deputy National Security Advisor for Combating Terrorism, who was tasked with operational coordination of combating transnational terrorist activities. To alleviate the internal confusion such a distribution of responsibilities could cause, NSPD-8 subordinated this individual to the Assistant to the President for Homeland Security as well as Assistant to the President for National Security Affairs.

In 2002, the Secretary of Defense approved a new doctrine separating "homeland security" from "homeland defense." This doctrine recognized a category of military activities that would occur within the homeland but which would be governed by the military chain of command as prescribed in the Goldwater-Nichols Act. These activities were defined as "homeland defense" and their scope is essentially to be determined at the discretion of the Secretary or the President. "Homeland security," on the other hand, was basically everything else that the department could do inside the homeland to support other federal agencies. The department also established U.S. Northern Command to better organize the resources of the department for various homeland defense and homeland security missions.

Even more significant changes occurred in early 2003 with the passage of the Homeland Security Act of 2002, which established the Department of Homeland Security, and the President's signing of Homeland Security Presidential Directive-5 (HSPD-5), which overhauled the federal approach to incident management. Replacing the bifurcated Presidential Decision Directive-39 framework with the single concept of "incident management," HSPD-5 was meant to resolve the ambiguity of authority inherent in separated concepts of "crisis management" and "consequence management." HSPD-5 designated the Secretary of Homeland Security as the "principal federal official for domestic incident management."[1] This means that the federal government can now always give the same answer to the "who's in charge?" question in an incident of national significance. Over time, the Department of Homeland Security will evolve into more of an operational integrator for domestic incidents, in Washington and in the field, although the Secretary of Homeland Security will never be formally in charge of all the different entities involved in responding to domestic incidents.

HSPD-5 also called for the promulgation of a National Incident Management System, which is essentially a template for multi-agency, multi-jurisdictional operational command and control in the field, and the National Response Plan, which will replace the Federal Response Plan and a number of other specialized plans. These are profoundly significant changes in the U.S. incident management system, particularly in the field, but their implementation is still underway and as yet the transitional problems are more apparent than the ultimate benefits.

Incident Management in General

The first point to understand about incident management in post-9/11 America is that the public's expectations of the federal government are exceptionally, indeed unrealistically, high. In a domestic incident of national significance, the federal government is expected by many not only to make no errors, but also to be virtually omniscient and omnipotent. Moreover, within the government, there is a chilling appreciation that one's every move could become the subject of endless official inquiry and public scrutiny. This is especially true in an incident that could in principle have been prevented. In recent official tabletop exercises that attempted to simulate realistic media "play" in a domestic terrorist incident, typically only a few hours would elapse before government spokesmen began to field questions about whom the President was going to hold responsible and fire.

The first point to understand about incident management in post-9/11 America is that the public's expectations of the federal government are exceptionally, indeed unrealistically, high.

Thus, the second key point to understand about managing terrorist incidents at the national level is that its most immediate and, in many respects, most difficult challenges have to do with communications. The public will thirst for information, not least because the entire population will experience the fear of being the victim of the next attack even as the physical effects of the terrorist attack are being experienced by only a small fraction of the population. This fact, which is not true in the case of natural occurrences such as tornados or hurricanes, puts an enormous premium on what the President and his senior-most officers say to the American people and how they say it. A bit of experience with managing complex national incidents teaches three iron rules:

1. First reports are usually inaccurate;
2. Accurate reports are typically embedded within significant uncertainty; and
3. The public, the media, and the government's communications specialists will demand information much faster than "the interagency" is prepared to provide it.

For these reasons, much of the incident management that occurs in Washington in the first hours of an incident will be dedicated to supporting the communications requirements of senior officials, who need to be extremely careful not to say anything that turns out to be incorrect due to the possible loss of life and public confidence that could result. This is especially true of the President, who will want to speak to the American people in the incident's first news cycle.

The most pressing question in the aftermath of a terrorist attack is going to be "Will they strike again?" To this central question, the federal government can never offer any definitive assurances. Because of al Qaeda's penchant for simultaneous attacks, the concern about follow-on attacks will weigh heavily on everyone involved in managing the incident. Responsible policy makers cannot assume that any attack is a one-off; they will have to devote a substantial portion of their time to maintaining vigilance. Although it has never occurred and decisions of this sort are made on a case-by-case basis, the U.S. government will likely raise the Homeland Security Advisor System level to "severe" ("red") in the immediate aftermath of a significant terrorist attack at home as part of its effort to prevent follow-on strikes and present fewer domestic targets.

An incident of national significance within the homeland will quickly reveal the incredible legal, political, and organizational complexity of the American system of government – much more so than will be the case in a major crisis abroad. The legal authorities of the federal executive branch inside the United States are substantial but confusing, uneven across various economic sectors and relevant policy areas, and often rooted in old statutes, court opinions, and executive orders. In any major domestic incident, America's federalism and limited government guarantees the involvement of a kaleidoscope of politicians (governors, Senators, Congressmen, mayors, state legislators, assorted county and municipal councilmen, etc.), non-federal public safety officials (police chiefs, fire chiefs, public health officers, etc.), and non-governmental leaders (corporate officers, union officials, experts, etc.) – all with ready access to a microphone or a TV camera and the right to say whatever they wish, irrespective of the preferences of the President or his subordinates. In this environment, the unilateral power and authority of the federal government is in fact quite limited. Effective incident management in a domestic setting requires the federal government to exercise leadership in more informal, politically sensitive, cooperative ways than is customary in the convenient chain-of-command that in theory controls the executive branch.

Incident Management in a Nuclear Weapons Scenario

In the event of the detonation of a no-notice nuclear weapon in an American city (a "nudet" in the vernacular of the business), evacuation of the downwind population is the only significant, immediate life-saving step available. Although the precise consequences of a nuclear detonation vary substantially with a large number of variables (yield, weapon type, blast location and elevation, environmental factors, etc.), the three basic effects are blast, thermal radiation, and nuclear radiation. Blast and thermal radiation are fast-acting, and their intensity falls off at the inverse square of distance or faster, making them essentially localized phenomena. Thus, there is little that can be done to save the people or property in the immediate vicinity of the nuclear detonation from the overpressure, building collapses, and conflagration. It is, however, possible to protect people from the effects of nuclear radiation if they remove themselves from the fallout zone before the radioactive particles reach them.

Given the short time available to effect an evacuation after a nuclear detonation, the only tool at the government's disposal is what it can say to the public in the first minutes after the blast. Specifically, can the government broadcast appropriate evacuation instructions to the affected areas quickly enough to make a difference? The two basic instructions are to move in a specific direction or to shelter in place until further notice. In general, the people in the center of the plume need to move out as quickly as possible if they are to avoid radiation exposure; the people on the edges of the plume may be better off sheltering in place; the people outside of the plume need to stay in place to avoid aggravating the congestion on the roads; and everyone needs to be told not to enter the plume. Once the government has spoken, the downwind population is basically on its own; it is not at all clear that local emergency response personnel will be able to offer appropriate assistance in the relevant timeframe.

In managing a nuclear attack, the key life-saving variables will be the speed and accuracy of the plume model that is provided *within minutes of the detonation;* the government's ability to translate this plume model into correct, easily understood movement instructions for the general public; and the government's ability to disseminate this message to the people in the affected area. The

greatest enemies of effective incident management in such a scenario will be time and indecision: the latter will be determined by the yield of the nuclear device and by wind speed, the former by the competence of the officials on duty in the first hour or so after the detonation.

The United States is, at the moment, not well prepared to manage a no-notice evacuation of this sort in the relevant timeframe. The plume modeling capability is ready and can be activated very quickly, but the federal government currently lacks the ability to generate and broadcast specific, geographically tailored evacuation instructions for all U.S. cities in the relevant timeframe. Moreover, a realistic field exercise of such a scenario is impossible, leaving the government with only tabletop exercises to work with, a decidedly second-best option.

The longer term consequences of a nuclear attack on a U.S. city are virtually inestimable.

The longer term consequences of a nuclear attack on a U.S. city are virtually inestimable. The evacuation, clean-up, and economic recovery of the affected area would be a major challenge, as would the long-term health care needs of the affected people, but these challenges would pale before the profound changes such a calamity is sure to trigger at home and in the world beyond.

Incident Management in Bioterrorism Scenario

For the purposes of incident management, the defining features of a bioterrorism incident will be delayed identification of the attack; enormous uncertainty about the scale and extent of the attack; a race against time to identify and treat infected individuals; widespread popular terror at an invisible, odorless, tasteless menace; and the certainty that there is no inherent limitation to production of bioterrorism agents once initial production capacity has been established.

The world has really experienced only one bioterrorist attack: the anthrax letters of October 2001. The management of this incident revealed a number of major deficiencies, several of which the U.S. government has taken major strides to correct. The United States now has a cadre of real experts on biological warfare and counter-measures that it will be able to draw on when needed. The United States has also invested billions of dollars in researching, developing, and producing a wide range of antibiotics, vaccines, and therapeutics, many of which can be airlifted on pallets to an attack site in a few hours. The government has deployed the first-ever atmospheric sensor system, called BioWatch, which operates 24-7 in most large U.S. cities, is highly sensitive, and provides important early warning possibilities. The government now has reasonably effective procedures and protocols for dealing with the still-relatively frequent "white powder" episodes and the like. And the government has developed a remarkable, largely classified bio-forensics capability, principally in response to the inability to identify the perpetrator of the October 2001 attacks.

There are, however, at least three major remaining problems in U.S. preparedness for a bioterrorism attack. The first, and perhaps most significant, is the limited capacity to perform prophylaxis on the scale and at the speed that will be required in a major bioterrorism incident. The United States currently has enough antibiotics and other drugs to treat more people than any terrorist could conceivably infect with a non-contagious, non-resistant, bacterial bioterrorism agent, such as anthrax or tularemia. Obviously, a contagious agent, particularly if aerosolized, could over-

whelm U.S. pharmaceutical stockpiles, while a resistant bacterial agent or a viral agent could essentially sidestep the stockpile. However, there are two interrelated operational complications for mass prophylaxis even in a non-contagious, non-resistant, bacterial bioterrorism scenario.

Demand for prophylaxis will far exceed actual infection. At the moment, no U.S. city is capable of distributing the medicines contained within the national pharmaceutical stockpile with the speed and efficiency that will be required to save lives in a large-scale, no-notice, symptomatically detected, aerosol attack involving a fast-acting bioterrorism agent such as anthrax. The reason for this deficiency is that the federal government has always relied upon state and local governments to provide "terminal distribution" for the medicines contained within the national pharmaceutical stockpile – that is, the transfer of the medicines from pallets at an airport into the bloodstream of potentially infected individuals. State and local governments have tended to assign responsibility for this task to their public health agencies, which in general have greeted the bioterrorism threat with great skepticism and have not taken seriously the need to prepare a distribution scheme for the stockpile that would be dramatically faster than that necessary for a naturally caused disease outbreak. These realizations, which have emerged only in the past year or so, have cast doubt on the appropriateness of the long-standing federal reliance on state and local agencies for the terminal distribution of the national pharmaceutical stockpile.

If the bioterrorism attack is a serious one, the government will quickly be confronted with a terrible decision – whether to withhold prophylactic medicine to scared citizens who want treatment but lack any medical evidence of exposure or infection.

This is not the end of the problem. The atmospheric-dispersion models that will be generated after the initial attack has been first detected will indicate a far larger potentially exposed population than is actually the case; all these people will be tapped to receive prophylaxis. Then, once news about the attack has been broadcast along with the fact that there is no inherent limitation to production of bioterrorism agents once initial production capacity has been established, people all over the country and indeed the world will start fearing that they will be the next victim of an imperceptible, deadly etiologic agent in the air. Many people, therefore, will make the individually sensible calculation that this risk is sufficient for them and their families to start taking a few antibiotics. If the bioterrorism attack is a serious one, the government will quickly be confronted with a terrible decision – whether to withhold prophylactic medicine to scared citizens who want treatment but lack any medical evidence of exposure or infection.

Tabletop exercises of such scenarios have suggested that decision-makers are likely to take the operationally unwise but politically expedient decision to supply the medicines to whoever wants them; certainly, it would take an unusually cold-blooded and steely elected leader to say "no" in such a situation. Once it is decided not to withhold medicine, stockpiles will evaporate quickly – leaving the country with little or no prophylactic reservoir to handle any follow-on attack.

The second major remaining problem in U.S. preparedness for a bioterrorism attack concerns movement restriction. It is likely that a major, aerosolized bioterrorism attack in a U.S. city will, once it becomes publicly known, trigger a chaotic and uneven evacuation of that city and possibly other cities as well. It is also likely that major commercial conveyance systems (airlines, trains,

buses, and ships) will spontaneously divert from the affected city, region, or country. At the moment, the U.S. government is more likely to be an observer than a manager of these rapid, large-scale changes in transportation patterns.

There are several reasons why this is so but the most significant is that the uncertainties in the early stages of a bioterrorism attack will be so vast that the government will frankly have no idea what to recommend to millions of different actors who will or could take to the roads, rails, waterways, or skies. The trouble is that the interactions of the various systems involved – atmospheric, geographic, transportation, psychological, immunological, logistical, etc. – are so complex that the government at this time simply lacks the capacity to generate correct movement instructions or correct movement restrictions for the relevant segment of the public in the relevant timeframe.[2] The government also lacks the ability to disseminate tailored movement instructions to people by area and, for all intents and purposes, to enforce non-consensual movement restrictions on land.

Finally, the government is ill-prepared to deal with the international dimensions of a bioterrorism scenario. This would be particularly true in a scenario involving an agent that could be treated by a vaccine or therapeutic contained in the U.S. national pharmaceutical stockpile, which is a unique global capability. If there is an anthrax attack in another country, that country is quite likely to immediately ask for U.S. assistance, i.e., the provision of prophylactic medicines from the U.S. stockpile. However, those medicines are a finite resource that might be needed to save the American civilian population. An even harder case would be the contagious viral agent smallpox. The United States possesses enough smallpox vaccine to vaccinate all 250-plus million Americans – but not many more people after that. If smallpox breaks out in, say, Turkey, the U.S. President will instantaneously be confronted with a truly no-win decision: protect all Americans from the dread disease by restarting a universal (American) vaccination program, in effect turning the United States into an immunological island while allowing the disease to run its course in the rest of the world; or jeopardize American lives by deploying the vaccine abroad in an effort to contain the outbreak in Turkey and save Turkish lives. Policy on issues of this sort has not been decided, or, at least, not written down.

Conclusion

So what can the U.S. government do to get better at incident management? In essence, four things:

- Sort out roles and responsibilities in sensible ways
- Acquire world-class expertise to support decision-making and public communication
- Acquire critical operational capabilities that can be deployed in relevant timeframes
- Practice

At this time, the United States has significant, and in some cases unprecedented, efforts underway in all four areas. Progress is, of course, slower than one would like in virtually every respect. Funding is not the rate-limiting factor; it is instead the limited knowledge. Years of experience and study have taught the federal government how to manage certain kinds of repetitive natural disasters, such as hurricanes, as well as certain kinds of man-made disasters, such as industrial accidents, financial crises, and wars. A major WMD attack on the homeland would be unprecedented, fearsomely complex, and utterly terrifying. The United States has not yet developed the vast new intellectual capital needed to proficiently manage such an incident.

Another, and indeed related, obstacle to more effective incident management is limited participation of policy makers at the highest level – that is, those individuals who will immediately surge into their command posts and operation centers to manage a major incident if it happens – in intellectual and operational preparation for national incident management. This is, to a certain extent, inherent in an exercise as dismal as incident management. The sheer horror of the scenarios, combined with their low probability of ever occurring, conspire to make most other activities a more attractive use of senior policy makers' time.

Nor is this an entirely illogical outcome. Time is the most valuable commodity possessed by any senior policy maker. Time to do real work – time that is not consumed by testimony, speeches, personnel matters, budget hearings, and the rest of the "in box" – is certainly the scarcest of all. So if a senior policy maker has a choice between spending his or her time on preparing to manage a nasty incident a home, on the one hand, or preventing a nasty incident at home, on the other, it is certainly arguable that he or she should spend as much time as possible on prevention. It is precisely this calculation that has led the Bush administration to attach primacy to prevention in all of its major strategies – the National Security Strategy, the National Strategy for Homeland Security, the WMD strategy, and the combating terrorism strategy. Incident management is a critical capability to develop, but we should never lose sight of the fact that once we have entered an incident management phase, we have already suffered our greatest failure.

Endnotes

1 HSPD-5 also modified the responsibilities of the Assistant to the President for Homeland Security, who was made responsible, together with the Assistant to the President for National Security Affairs, for "interagency policy coordination on domestic and international incident management." This is a highly elastic formulation; its practice will evolve as the Department of Homeland Security matures and as the many interagency frictions associated with the emergence of this new Department are resolved.

2 In a serious bioterrorism scenario, it is virtually certain that the right course of action for an individual person, vessel, or company will diverge from the right course of action for the affected region as a whole. For instance, while it may make sense for a person on the fringes of a bioterrorism plume to flee the area, from the region's point of view it would probably be better for that person to shelter in place, thus lessening the congestion on the roads and making it easier for people in the core of the plume to exit and for emergency workers to enter. Similarly, while it may make sense for a trucking company to halt shipments in a city that has experienced a bioterrorism attack, many of those trucks would be carrying urgently needed supplies for the mass medical operations that would be occurring in that city.