

Bioterrorism, Fear, and Public Health Reform: Matching a Policy Solution to the Wrong Window

During the 1990s, terrorist actions using biological weapons and the fear that rogue states possessed such weapons placed bioterrorism on the political agenda, a policy window widened by the September 11 attacks. Advocates for improving the U.S. public health infrastructure attempted to use this window to obtain the resources necessary for modernization. This article examines those efforts and identifies significant problems arising from a mismatch between the goals of public health policy entrepreneurs and the policy window used to address them. By defining bioterrorism as a security rather than a public health issue, policy entrepreneurs squander the opportunity to institute broad-based reforms that would improve not only the ability to manage a terrorist incident, but also meet other public health needs. The bioterrorism program proves a useful case study in how the goals of policy entrepreneurs can be displaced by attaching policy preferences to the wrong policy stream.

In 1910, M.J. Roseneau argued that fear is the most useful tool of public health because it maintains the public's respect for the threat of epidemic disease. In the late twentieth century, that fear was lost to advances in medicine and public health which eliminated smallpox, discovered effective antibiotics and vaccines, and made sanitation improvements that, together, reduced deaths from infectious disease by 90 percent. By the late 1980s, public health was subjected to significant social and cultural discounting, with subsequent neglect and deterioration in capabilities (Fee and Brown 2002; Berkelman et al. 1994). By the early 1980s, states were ceasing tuberculosis surveillance at a time when drug-resistant strains were arising. Over the next two decades, infectious disease mortality rates, after discounting for the AIDS epidemic, rose 22 percent (Drexler 2002, 6–7). In 1988, the Institute of Medicine warned of the risks of deterioration and suggested a need to rebuild the system (Committee for the Study of the Future of Public Health 1988). In 1992, it further warned that the public health system had continued to deteriorate, and emphasis needed to be placed on the prevention of infectious disease (Lederberg 1992).

Kingdon (1984) describes a policy process in which discrete streams of problems, policies, and political actors are coupled in “policy windows,” that is, critical moments when policy entrepreneurs can successfully match problems to

policy solutions. By the mid-1990s, public health advocates had developed solid technical proposals to upgrade the public health system, but they failed to make a compelling political case (Foreman 1994). The window had yet to open. That began to change in the late 1990s. By then, the policy stream for advancing these goals contained two proposed policy solutions (table 1). Both used issues with the potential for exploiting public unease to advance the building of public health infrastructure. The first—based on previously unknown diseases such as AIDS and Ebola, which emerged as rates of known epidemic diseases such as tuberculosis were growing—emphasized the need for non-disease-specific improvements in the infrastructure for surveillance, research, training, and prevention of infectious diseases (CDC 1998; Osterholm 2000).

The second strategy focused on using the fear of terrorist attacks with weapons of mass destruction to piggyback structural improvements onto a program to respond to threats from biological weapons (Osterholm 1999). In 1999, prompted by Aum Shinrikyo's use of the nerve agent sarin in Tokyo in 1995 and subsequent revelations the group

George Avery is a doctoral candidate in health services research and policy at the University of Minnesota School of Public Health and an instructor with the University of Minnesota–Duluth Psychology Department. He served for 10 years with the Division of Public Health Laboratories, Arkansas Department of Health, and holds a master's degree in public administration from the University of Arkansas–Little Rock. **E-mail:** aver0042@umn.edu.

had attempted to use anthrax spores, the U.S. government launched an antibioterrorism initiative. This program addressed issues related to infectious disease control and surveillance, but in the context of responding to an attack with infectious agents that had historically been developed as military weapons.

This article proposes to examine the differences, strengths, and weaknesses between the two approaches and discuss which is superior in terms of improving the public health response to infectious disease. Additionally, the role of the environment in shaping the adoption and implementation of a policy option will be reviewed.

Evaluation Criteria

This study examines the implementation of bioterrorism-preparedness policy using publicly available documents on implementation and performance to evaluate the effectiveness of the program in meeting public health and civil defense goals.

First, the proposals are examined in terms of the risk of the events each was developed to respond to. In terms of resource allocation, it is anticipated that preparation for high-risk events will be more efficient than low-risk events of similar consequences. Similarly, the breadth of events that can be handled by each proposal is examined. All other criteria being equal, a system that can handle a wider range of risks is likely a more efficient tool for utilizing public health resources than a narrowly focused program. However, a program that is narrowly focused on addressing a high-probability, high-impact event may be more effective than one addressing a wide variety of low-risk events.

Second, we look at evidence related to the effectiveness of the approaches. How well is each proposal supported by evidence resulting from public health practice? What results can we expect from the implementation of these policies? As part of this, the proposals are examined in terms of the appropriate roles of federal, state, and local governments, and private-sector agencies. This study will examine how the programs interact or reshape these roles, as well as how the involved agencies are coordinated.

Inherent in this analysis is a focus on implementation. As Pressman and Wildavsky (1973, 143) note, "The great problem ... is to make implementation a part of the initial formulation of policy. Implementation must not be conceived as a process that takes place after, and independent of, the design of policy." A policy is only a verbal construct until it is implemented. Implementation translates this verbiage into a concrete, observable policy. Thus, one needs to consider how the responsible agencies are likely to implement the policies, and how the policy and organizational climates shape this implementation. How does defining the problem as a terrorist incident cause a differ-

ent response than defining it as a public health problem? How does this relate to policy effectiveness and efficiency?

Program Differences and Similarities

The two programs share many similarities (table 1). Both include elements to improve surveillance, laboratory capabilities, infectious disease training, and preparation to respond to an outbreak. Both would fund the creation of electronic disease reporting systems and use of syndromic data from health-care providers. Both include infectious disease training for providers and for state and local health officials. Both include research into vaccines and new drug development, and proposals for developing stockpiles of drugs and medical equipment as surge capacity for a large event. Both include enhanced food supply surveillance.

The major defining difference is in focus. Wildavsky, in *Searching for Safety* (1988), identifies two approaches to risk management—anticipation and resilience. Anticipation attempts to identify and prevent problems, while resilience attempts to build the capacity to handle unanticipated problems. The bioterrorism-preparedness program is an example of the anticipation strategy, focusing on the specific threat of a terrorist attack involving military biological weapons—in particular, smallpox, anthrax, plague, tularemia, brucellosis, and Q fever. As a result, laboratory improvements focus on diagnostic tests for these specific diseases, stockpiles are built on treatments for these diseases, and response is based on an emergency-management model similar to that used for a natural disaster or industrial accident rather than an epidemic. Training focuses on emergency responders rather than health-care providers. Because of the implications of terrorism on national security policy, the bioterrorism proposal involves more agencies, and the program is focused on federal rather than state and local roles. Rather than building local surge capacities, centralized stockpiles and response teams are created. A police function is as important as the public health protection function.

In contrast, the emerging infections strategy relies on a resiliency model which assumes that, because we do not know the specific threat that will occur, building the capability to respond to a variety of threats is of greater utility. Laboratory upgrades focus on the capability to respond to a variety of unusual events. Training focuses more on public health and health-care providers than on emergency managers and responders. Surge-capacity development focuses on both local and national levels. Coordination with nonhealth agencies is part of the planning process, but managing the public health aspects of an event is the primary concern, and resources that are allocated to security agencies in the anticipatory model are put into the public health and health care sectors.

Table 1 Comparison of Bioterrorism and Emerging Infections Proposals

Item	Bioterrorism proposal	Emerging infectious disease proposal
Disease focus	Limited list of agents weaponized in military programs such as: ¹ <ul style="list-style-type: none"> • smallpox • anthrax • plague • tularemia • brucellosis • Q fever 	Broad preparedness for unusual disease events including: <ul style="list-style-type: none"> • antimicrobial resistance • food-borne disease • waterborne disease • arthropod-borne and zoonotic diseases • transfusion and blood product safety • chronic diseases caused by infectious agents • problems of immunocompromised patients • neonatal disease and diseases of pregnant women • disease transmission though travel
Laboratory preparedness	Technology upgrades for anthrax, botulism, plague, tularemia, brucellosis	Broad-based upgrades for public health surveillance and diagnosis of infectious diseases
Surveillance	<ul style="list-style-type: none"> • Enhanced Surveillance project—use of ED data for syndromic detection of events involving target agents • National Electronic Surveillance System—broad-based integrated electronic reporting system • Communications infrastructure improvements within the public health system • Improved food inspections for select agents 	<ul style="list-style-type: none"> • Enhanced population-based surveillance • International network for antimicrobial surveillance • Improved electronic reporting infrastructure • Improved food-safety inspections • Epidemiology and Laboratory Capacity Program (ELC)(30 states involved 1995–98) • Emerging Infections Program • Provider based syndromic surveillance
Training	Training for emergency responders and local and state health departments	<ul style="list-style-type: none"> • Improved training for epidemiologists and laboratorians • Improved training in infectious diseases for health care providers
Response preparedness	<ul style="list-style-type: none"> • Central national drug stockpiles targeted at selected diseases. Response time, minimum 48 hours • Multiple agencies with response role—lack of clearly defined coordination means • Revaccination for smallpox • Training for metropolitan emergency responders in biological warfare agents • Vaccine and drug development for targeted agents 	<ul style="list-style-type: none"> • New program for vector control • Prevention guidelines coordinated with providers and managed care organizations • Infectious disease outcome indicators with feedback to hospitals and managed care organizations • Vaccine and antimicrobial development based on risk assessments • Develop social and behavioral interventions for prevention of infectious diseases • Planning and coordination for complex events, including but not limited to bioterrorism <p>Build surge capacity at the state and federal levels, including drug stockpiles</p>

¹See biological agents and diseases downloaded from <http://www.bt.cdc.gov/Agent/agentlist.asp>.

Bioterrorism Program History

From 1970 to 1998, 415 potential chemical or biological terrorism incidents occurred in the United States. These included a 1970 attempt by the Weather Underground to obtain biological agents from the U.S. Army Medical Research Institute on Infectious Diseases; a 1991 plot by the Minnesota Patriots Council to attack government officials with ricin; and a 1998 case in which an antigovernment activist threatened to use legally acquired plague cultures against government installations. In 1984, the Rajaneeshee cult contaminated restaurant salad bars in The Dalles, Oregon, to influence a local election, resulting in several hundred illnesses (Torok et al. 1997). These incidents have led to a belief that two important prerequisites for successful bioterrorism—vulnerability and capability—were in place (Siegrist 1999). This belief was reinforced by the 2001 anthrax attacks, which caused 22 cases and five fatalities in seven states (Jernigan et al. 2002).

The belief that hostile entities were able to obtain weapons of mass destruction and that the United States was vulnerable to such attack resulted in initiatives to prepare

the country. After the Persian Gulf War, Iraq admitted to having a variety of biological weapons, including anthrax, ricin, and others. The Iraqis' failure to comply with agreements to destroy this stockpile served as the *causis belli* for the 2003 war; it also led to the realization that other state sponsors of terrorism had active biological warfare programs, indicating that a capability exists for transferring these weapons to terrorists (Alibek and Handelman 1999). The Aum Shinrikyo and other incidents indicated that weapons could be acquired without government assistance. As a result, the United States began to examine the possibilities of an attack. In 1993, debates at the Centers for Disease Control and Prevention (CDC) about the destruction of remaining smallpox virus stockpiles were jarred by revelations that the Soviet biological weapons program had weaponized the virus (Garrett 2000, 482–83). In 1995, Presidential Decision Directive No. 39 (PDD-39) directed federal agencies to plan for bioterrorism defense, and the 1996 Defense against Weapons of Mass Destruction Act created a domestic preparedness program for training and assisting state and local agencies.

The first efforts to address the threat of biological warfare occurred during the 1950s, when Cold War concerns led to the creation of the Epidemic Intelligence Service at the CDC. Although this had a long-term impact in developing the CDC, it was also the beginning of a dramatic decline in resources for state and local health departments, weakening the overall strength of the public health system (Fee and Brown 2001). Except for research conducted by the Army Medical Research Institute on Infectious Diseases, little was done for biological civil defense between the 1950s and the 1990s. The Reagan administration created the National Disaster Medical System, a voluntary network of hospitals and providers, to assist local providers when a catastrophe overwhelmed state and local capacity. The Federal Emergency Management Agency (FEMA), under the Disaster Relief Act of 1974 as amended by the Stafford Act of 1988, administered several federal disaster assistance programs (Smithson and Levy, 2000, 114–16). There are indications this authority would not apply in the event of an unconventional terrorist attack (McKinney 2000).

Starting in 1995, the federal government initiated programs to establish a response capability for bioterrorist incidents. PDD-39 set priorities for antiterrorist activity and delineated responsibilities for such events, with the FBI holding crisis-management responsibilities and FEMA managing the consequences. In 1996, the Defense against Weapons of Mass Destruction Act authorized the army to train first responders from the 120 largest U.S. cities, established response teams in the Departments of Defense and Health and Human Services, and called for joint federal, state, and local training exercises. The Anti-Terrorism and Effective Death Penalty Act of 1996 authorized the Department of Justice to make training grants to local first responders and required the CDC to regulate access to potential biological weapons. In 1998, the White House followed PDD-39 with PDD-62, targeted at weapons of mass destruction, which continued the Defense and Justice Departments' efforts, established the Public Health Service as the lead agency for medical response for bioterrorism and charged it with creating medical supply stockpiles, and called for the creation of rapid-response teams without specifying a responsible agency (Smithson and Levy 2000, 118–22).

By FY2001, the federal budget request for unconventional terrorism preparedness had reached \$1.4 billion, with \$166 million allocated to health and human services (Center for Civilian Biodefense Studies 2000). For FY2003, the budget request totaled \$5.9 billion (Dalton 2002). The health and human services program focused on five program areas: (1) restrictions on access to infectious agents; (2) improvements in state and local surveillance capabilities; (3) improved response capabilities; (4) medical stock-

piles; and (5) vaccine and rapid diagnostics research (Hamburg 1999). For the Department of Health and Human Services, \$96 million was allocated to improving local capacity (Smithson and Levy 2000, 125). In 1999, the CDC granted \$41 million to state and territorial health departments, as well as to the cities of Los Angeles and New York, to improve surveillance, communications, diagnostics, and training (Lillibridge, Bell, and Roman 1999; Center for Civilian Biodefense Studies 1999). Currently, this program focuses on anthrax, smallpox, tularemia, plague, botulism, and viral hemorrhagic fevers, with lesser emphasis on brucellosis, Q fever, glanders, typhus, melioidosis, psittacosis, and biotoxins such as ricin.

Risk

The Association of State and Territorial Health Officers argues that effective bioterrorism response requires general improvements in the public health infrastructure (Bryan and Fields 1999). Both program supporters and opponents agree. Effective postattack management of bioterrorism involves the traditional public health responses of event recognition, intervention, preventing further casualties, and public reassurance. The actual goals of the Health and Human Services Department's bioterrorism programs include strengthening the public health infrastructure. As one proponent observed, "Over the last 20 to 25 years, efforts to bring about structural reform in state and local governments and in local public health departments have eroded. Efforts by Congress to fund the bioterrorism initiative may have a dual effect: they may not only improve our ability to respond to a bioterrorism incident, but also may strengthen state and local health departments" (McCann 1999).

Other advocates make the same argument. Joseph McDade (1999) of the CDC argues that improvements targeted by the bioterrorism program benefit the public health system, helping it to manage other infectious diseases by rebuilding capacity that eroded in the 1960s and 1970s.

Critics argue the trickle-down effect from the focused bioterrorism program is less effective than general infrastructure improvements and may divert resources from general public health efforts that have greater impact (Geiger 2001). Laboratory improvements, for example, focus on expanding the use of sophisticated techniques such as pulsed phase gel electrophoresis, but only for targeted diseases. Surveillance improvements also focus on the same agents—training emergency room physicians, for example, to consider inhalational anthrax when presented with flu-like symptoms, or to recognize the difference between measles and smallpox. Although useful in preventing serious casualties in the event of exposure to such an agent, as in the 2001–02 anthrax incidents, critics argue the prob-

ability of such an attack remains so low that dedicating extensive resources to specific rare diseases is less effective than general training and surveillance (Sidel, Cohen, and Gould 2001).

Which program is best depends on the magnitude of the risk—the likelihood of a bioterrorist attack occurring and the magnitude of the damage from attack. Before the September 11 attacks, many proponents had argued the probability of an attack was low, but that, depending on the agent, the likelihood of significant damage (upwards of 1,000 casualties) was high (Henretig 2001). On the other hand, the Central Intelligence Agency and the Defense Intelligence Agency had rated the probability of an attack occurring as high (Anderson 1998). There is doubt whether a non-state-sponsored organization can carry out a large biological attack. Significant technical barriers exist to preparing and delivering agents to cause mass casualties (Smithson and Levy 2000, 37–56). Aum Shinrikyo shifted from anthrax spores to chemical weapons because of the inability, even with a sophisticated, well-funded program, to inflict casualties using anthrax (Roseneau 2001; Block 2001). Proponents of a dedicated bioterrorism program argue the barriers are eroding, with the growing likelihood of an attack (Tucker 1999). Evidence from previous bioterrorism attempts is mixed. The 2001 attacks resulted in 22 infections with five deaths (Jernigan et al. 2002). The 1984 Oregon incident resulted in 751 cases, but no fatalities, and involved an agent (salmonella) that was not on the priority list (Tucker 1999). The worse terrorist incident in American history, in contrast, cost more than 3,000 lives using hijacked aircraft rather than chemical or biological weapons.

The casualty estimates on which the current policy is predicated are based on larger, more sophisticated attacks. The 2001 “Dark Winter” exercise, for example, involved three state attacks with smallpox and projected 16,000 cases in 25 states and breakdowns in civil society (Roman 2002). The 2000 FEMA/Department of Justice “Topoff” exercise involved a large attack involving pneumonic plague in a major metropolitan area (Brownlee 2001; Katz 2002). A 1998 exercise involved a “superflu” bug, killing more than one million (Garrett 2000, 536). The May 2003 Topoff 2 exercise centered on a multistate attack with both radiological and military biological weapons, delivered by a fictional nongovernmental terrorist organization (Walsh and Mintz 2003).

In an economic impact analysis to support the current program, Kaufman, Meltzer, and Schmid (1997) of the CDC found that annual expenditures of \$140 million–\$200 million on bioterrorism prevention represent an actuarially fair premium, under a maximum-cost scenario, reduction-of-incident probability of over 90 percent, and treatment within 24–48 hours. This is based on an anthrax attack

exposing 100,000 people, with 32,875 deaths, and it does not include ancillary benefits to the public health infrastructure. Within this estimate, which uses scenarios far more severe than have been historically observed, the program funded at 2000 levels is marginally efficient, assuming that prophylaxis and treatment is rapidly initiated. It is inefficient at 2002 funding levels.

An assessment of the existing program’s cost-effectiveness depends on accurate forecasts of the probability and scale of an attack, response efficiency, and the extent to which the program provides other public health benefits. Presently, based on the reality of past bioterrorism incidents compared to theoretical incidents, it does not appear the reality is adequate to justify a program dedicated exclusively to bioterrorism preparation, not considering issues of program effectiveness. Falkenrath, Newman, and Thayer (1998, 27–96), advocating preparedness, note that little information exists on actual risk, and, although the risk is likely increasing, there are significant technical and psychological barriers that would keep most state and nonstate actors from using weapons of mass destruction.

There are no data available on returns from using bioterrorism funds to strengthen the general public health infrastructure. At least one estimate indicates that, with the funds from the bioterrorism initiatives, adequate resources exist for the public health infrastructure to meet its goal of protecting the public health, if allocated correctly (Katz 2002). Infectious diseases remain the largest global cause of death (Berkelman and Hughes 1993), and almost all of these deaths result from “natural” epidemics. Sidel, Cohen, and Gould (2001) note that the United States suffers 325,000 annual hospitalizations and 5,000 deaths from food-borne illness alone, comparable to a low-probability, large-scale bioterrorism attack. Smithson and Levy (2000) evaluated the current efforts and finds that a significant problem is the identification of real versus hyped risks, necessary for resources to be allocated to achieve the greatest impact. If general improvements can prepare the public health system for a bioterrorism incident, then such investment would be more effective and efficient in maintaining public health than a system targeted at specific agents with a trickle-down improvement to the overall infrastructure.

The question, therefore, is whether the improvements suggested by the emerging infectious diseases proposal can deal with bioterrorism. The original CDC proposal (1998) contains explicit provisions for interagency coordination to handle the security aspects of a bioterrorism incident. Richards, O’Brien, and Rathbun (2002, 722) suggest, “The best way to manage the risk of bioterrorism is not to expend precious resources and political credibility on low frequency events, such as bioterrorism, but to focus on day to day public health functions, i.e. channel public and leg-

islative fears about bioterrorism to fears about everyday public health.”

The basic tasks of dealing with bioterrorism remain those of public health—identifying unusual occurrences and causes of disease and intervening to alleviate the situation. It is difficult to distinguish between natural and bioterrorism events. The Oregon attack went unrecognized as bioterrorism for well over a year. Treadwell et al. (2003, 96) note that “except for the most blatant violations of natural principles, bioterrorism will continue to remain difficult to differentiate from naturally occurring outbreaks.” Similarly, Ashford et al. (2003) of the CDC, in a retrospective study of potential bioterrorism events, note similarities in the presentation of natural and intentional outbreaks and that “intentional contamination may resemble naturally occurring outbreaks, may spread slowly through the population, and may involve endemic pathogens” (517).

In summary, a narrowly focused bioterrorism program is an efficient allocation of resources only under worst-case risk assumptions. In almost any scenario, the risks addressed by the emerging infections proposal are greater than those addressed by the bioterrorism program; although both encompass the bioterrorism threat, the emerging infections proposal includes systemic reforms to address other infectious diseases.

Implementation Issues

The first test of the current preparedness program occurred with the small-scale anthrax attacks in 2001. Significant problems appeared, even though the attack involved an agent the system is specifically designed to respond to. Cooperation between the FBI and the CDC was limited, and the CDC never had access to the contaminated letters, resulting in improper control measures at the Brentwood, New Jersey, post office and leading to additional casualties. The FBI had the agent analyzed by the Army Medical Research Institute on Infectious Diseases rather than the CDC—the agency primarily responsible for the public health aspects of bioterrorism—and did not do so until further infections had occurred (Siegel 2002; Deqn et al. 2002). Contributing to the problem was the fact that the FBI, lacking public health expertise, did not respond properly to a situation that did not fit its script of how a terrorist incident would look (Drexler 2002, 266). This was not a new issue. During the 1994 “Mirage Gold” nuclear terrorism exercise, the FBI agent in charge of the response was unwilling to share information with other agencies, and the FBI failed in 1995 to notify local authorities of a nerve agent threat against Disneyland (Falkenrath, Newman, and Thayer 1998, 10–11). The Topoff exercise identified coordination as a problem in bioterrorism-response capability. The lack of a clear chain of responsibility seriously hin-

dered public health officials in dealing with the epidemic, resulting in further casualties and social disruption (Brownlee 2001). The response to a real incident, a year later, revealed the lessons had not been absorbed.

The current bioterrorism program tries to address some of these problems. Funding is provided for laboratory upgrades, surveillance, planning, and communications between local, state, and federal health authorities. This is targeted, however, at terrorist incidents involving traditional military biological weapons. CDC training for laboratory staff focuses on diagnostics for the targeted agents. The danger exists that the improvements will be compartmented rather than applied to broader risks. Public organizations tend to be constrained by procedures adopted to meet contextual considerations (Wilson 1989, 133). Thus, the context of bioterrorism preparedness should not be limited to targeted agents. For example, a focus on the targeted agents would have been of little help in the Oregon incident, as salmonella is not targeted. Knott and Miller (1987), discussing bureaucratic dysfunctions, note a tendency for goal displacement in agencies:

Having accepted a set of standard operating procedures by which to achieve an organizational goal ... an individual in an organization will not rethink this system repeatedly; he will take the SOPs as given—as premises for decision—in order to concentrate on the day-to-day issues. This means that the individual will not concern himself with the original design of the organization, but will rather be satisfied with following the means that had at one time been determined to be appropriate for the goal, the individual will thus come to pursue these means as if they were goals. (172)

Pentland and Rueter (1994) find that patterns in organizational action arise even in nonroutine work through the structural features and cognitive models of the participants. Cosmides and Tooby (1994) state that “cognitive specializations determine what inferences will be triggered by a situation and what kinds of information will be attention grabbing, memorable, learnable, communicable” (332). Thus, it is expected that focusing attention and training on specific agents is likely to distract from considering disease events, natural or terrorist, that do not fit the established guidelines of what to look for, reducing the utility of the program for both antiterrorism and general public health purposes.

In the context of terrorism, crisis management—including intelligence gathering and criminal prosecution—is generally a federal responsibility, while consequence management is a state responsibility that arises, like other public health functions, from state police powers. In a bioterrorism event, the lines are muddled. Even in a well-defined case like the 2001 attacks, jurisdictions were crossed and

poor cooperation even among agencies at the same level of government exacerbated the problem. In an attack that is not distinguished from a natural outbreak, the confusion is likely to be greater.

This poses a threat in two ways. First, the appropriate role of actors at different levels of the federal system needs clarification. Because responsibility for threats to public health is a traditional state responsibility, and federal involvement is generally limited to research and support of state programs, the proper level of management for infectious disease incidents seems to lie at the state and local level. However, as a national and internal security issue—as bioterrorism has been defined since September 11, 2001—it is a federal responsibility.

Constitutional limits exist on federal power to act during a bioterrorism incident. The 1877 Posse Comitatus Act, for example, limits military units to assistance in domestic emergencies when requested by state agencies, but it forbids civil law enforcement (Choo 1999), making the proposed role of the military in managing an event possibly illegal. A further complication is the range of federal agencies involved in bioterrorism. For example, even when state agencies are willing to submit to a federal lead, during the 2001 anthrax case, competing demands came from the FBI, CDC, Postal Service, and Army experts brought in by the FBI (Wise and Nader 2002).

State and local laws differ between jurisdictions and may be inconsistent with emergency needs. Minnesota, for example, requires separate court orders for each person quarantined, a major hurdle in an event involving a transmissible agent (Wise and Nader 2002). As a result, federal bioterrorism managers seek a uniform set of powers, including censorship of the media, liberalized search and seizure rules, and the power to compel civil servants and medical personnel to work, which are in violation of the First, Fifth, and Thirteenth amendments to the Constitution (Wise and Nader 2002) and considered by many to threaten the balance between security and liberty (Kayyem 2001). The Model State Health Powers Act proposed by the CDC (Gostin et al. 2002), which focuses on bioterrorism, drew significant criticism for exceeding reasonable bounds in compromising civil liberties (Kincaid and Cole 2002; Bayer 2002). Potential public distrust as a result of compromised civil rights is cited as a threat not just to bioterrorism programs, but to public health in general (Annas 2002). Etzioni (2002) criticizes the Model Act for emphasizing uniform distribution of burdens, noting that, regardless of how distressing the differential impact is, effective response needs to be adapted to the situation, and the burden resulting from an incident will necessarily fall unequally on the population.

Second, the problem definition shapes its perception, the agencies involved, and organizational perceptions of

which procedures are appropriate to manage it. Defining the problem as a security issue typically involves more agencies than defining the problem as a public health issue, and those organizations have different assumptions, as the 2001 anthrax event demonstrated. In that case, failure to prioritize public health aggravated the problem.

Among other issues, security and law enforcement agencies tend to compartmentalize information, which may keep data from those managing consequences. The new Department of Homeland Security, with a key role in bioterrorism planning and civil defense, is already showing tendencies toward compartmentalization, excluding many without existing security clearances from planning, and demonstrating little understanding of the integration of civilian entities into operations (Waugh and Sylves 2002). As Moynihan (1998) notes, a culture of openness in government, even in security affairs, improves efficiency by emphasizing analysis and full exploitation of information. Similarly, 't Hart, Rosenthal, and Kouzmin (1993) argue that in crisis situations and in preparing for crisis, centralized control is often nonoptimal, reducing the ability to apply expertise to the control center. In bioterrorism, the health aspects of consequence management demand information sharing in order to include those with health expertise in the decision process. The resiliency-based emerging infections proposal includes planning and coordination with security authorities for bioterrorism, but it focuses on the public health aspects. This is consistent with the actual presentation of such incidents, where the public health problem is recognized (and managed) before recognition as bioterrorism, triggering legal and security responses.

In the post–September 11 environment, when at war with a power known to support terrorism and known to have developed and used chemical and biological weapons, there is strong psychological and political incentive to put bioterrorism programs into the same security rubric as programs addressing traditional antiterrorism, which may not be optimal given the inherent public health aspects. A car bomb is an incident at a point in time and space, whereas a tularemia attack is an ongoing crisis spreading to new victims as time progresses, and may not be identifiable as terrorism. As is often noted, bioterrorism is a public health crisis until evidence mounts that it is something more. The use of anthrax by Aum Shinrikyo was discovered only after police raided cult facilities after the group's use of a nerve agent on the Tokyo subway. It is impossible to separate preparedness from the general public health system without perfect knowledge of the identity, intentions, and capabilities of potential terrorists, and, were that available, public health involvement would not be required.

Critics argue that, in order to avoid worst-case scenarios, the executive and legislative branches have authorized virtually any program claiming a tie to antiterrorism (GAO

1999; National Commission on Terrorism 2000; Smithson and Levy 2000, 288–98). Terrorism preparedness is something no one can argue against and survive politically, yet it can cause considerable political damage in the post-event incrimination phase if an event does occur. As Wilson (1989) observes,

... government executives often cannot take credit for accomplishing agency goals because goals are so vague or progress toward them so difficult to achieve (much less measure) that there is no basis for persuasively claiming credit. But these executives are always vulnerable to criticism. If that vulnerability can be reduced, if members of Congress, interest groups, and journalists cannot levy a plausible criticism against an agency, then these outsiders are deprived of an important means of asserting power over an agency. As a consequence, its autonomy is increased. (192)

In developing the bioterrorism-preparedness program, the interplay of existing (mainly federal) government agencies, Congress, the media, and a handful of policy entrepreneurs such as Michael Osterholm and David Henderson shaped the political environment. Before 2001, the major roadblock to improving the public health system was “simple indifference born of competing priorities” (Foreman 1994, 154). Congress and the presidency, particularly after the September 11 actions, need to show they are acting to protect the nation from further catastrophic terrorism. Agencies operate in an environment where there is every incentive—budget resources, self-protection, etc.—to show they *can* play a role in defending against bioterrorism. Policy entrepreneurs, many who were active in seeking public health reforms, used the window of opportunity to seek increased funding for their policy goals, but only in the context of that window. This is the historical pattern of public health reform—using anxiety and crisis to obtain system improvements. Historically, this has allowed short-term priorities to displace long-term needs, failing to generate sustained support for public health (Fee and Brown 2002). Thus, Calvert’s (1985) model of a rational actor maximizing utility by choosing biased over unbiased information holds. Unbiased estimates of threats and needs lead to uncertainty and promote inaction, leaving actors vulnerable to repercussions from failure. Accepting information biased toward the worst-case scenario—the mass-casualty biological weapons attack of military sophistication and the killing of thousands—justifies intervention. This leads to resource acquisition and the protection of autonomy from other actors who might encroach on agency turf in the event of inaction. In the Kingdon model, problem definition depends on the availability and political acceptability of a solution (Travis and Zahariadis 2002). A key as-

sumption in implementing policy is that policy makers share a vision of how to operationally define a policy at the implementation stage, a questionable assumption with multiple actors defining the problem (deLeon and deLeon 2002). Unfortunately, civil biodefense was dropped into a security environment that is unfriendly to the public health mission, where national security leaders fail to understand that the consequence of biological attack is the classic public health problem, an epidemic (Drexler 2002, 267).

The result is a proliferation of programs, jumbled jurisdictions, and a focus on addressing the worst case over the likely case. As Pressman and Wildavsky (1973, 134) note, “Everyone wants coordination—on his own terms.” Tobin (1986) and Eads and Fix (1984) find that in such an environment competing administrative priorities, limited resources, distrust, and misunderstanding limit intergovernmental cooperation. The result is a series of programs addressing a limited potential problem, but poorly.

The emerging infections model clarifies the lines of authority. Primary authority for an infectious disease crisis lies with public health authorities, with involvement by law enforcement and security agencies after an outbreak is identified as a likely terrorist attack. This ensures the focus remains on protecting health. In the United States, the leadership and coordination role belongs to the federal Centers for Disease Control and Prevention, with implementation at the state level. The CDC has been cited as the best agency for this role, not just at the national level, but also at the international level considering weaknesses at the World Health Organization (Henderson 1993). The agency has widespread credibility in the public health community, and, with the appropriate use of requirements and adequate funding support, the ability to organize change in state health departments. Given that disease can cross jurisdictional boundaries, federal leadership is proper and should be exercised by an agency that is defined by a public health mission.

The emerging infections proposal, as outlined, is sparse in addressing evidence handling and other legal issues. Successful implementation would mean training health care workers, laboratorians, and epidemiologists in evidence handling and custody procedures. This is not insurmountable, as those elements already exist in some public health regulatory and sanitation programs. One aspect of the bioterrorism program that has potential for the emerging infections model is the use of intelligence agencies to collect surveillance data on emerging threats (Johnson 2000, 72–91). The utility of this capability requires overcoming organizational biases in the intelligence agencies toward secrecy, compartmentalization, and creating a sense of importance for information in the intelligence community. Such a change would be a formidable task at best.

In summary, the focus on bioterrorism results from political pressures that create a climate in which political actors must act to show they are addressing a threat. This creates an environment where security and law enforcement agencies are given an outsized role in addressing public health problems, but they may have organizational priorities incompatible with health needs. Thus, interorganizational conflict is almost certain in a crisis, and response pathways are shaped by conflicting demands from these agencies. Thus, we anticipate, as the evidence suggests, that the program's ability to respond to the public health problems of bioterrorism will be handicapped, and the ability to respond to nonterror events will be constrained by structures imposed by security concerns.

Effectiveness

As noted, the bioterrorism preparedness program faced its first challenge as a result of the 2001 anthrax attacks and demonstrated serious weaknesses, despite involving a target agent. Interagency cooperation was limited and improper control measures implemented as a result, produced additional casualties. The FBI turned samples over to a military agency, bypassing the agency with primary legal responsibility for public health, and neither USAMRIID nor the FBI tested for seepage until further infections had occurred (Seigel 2002; Deqn et al. 2002). This was not a new issue. The Topoff exercise of the previous year had identified coordination issues as a serious issue in the bioterrorism response capability. Lack of a clear chain of responsibility seriously hindered the ability of public health officials to deal with the epidemic side of the scenario, resulting in additional casualties and severe social disruption (Brownlee 2001). The response to a real incident, a year later, revealed that the lessons had not been absorbed.

The current public health system has significant deficiencies that prevent it from adequately responding to bioterrorism or to other epidemics. According to the General Accounting Office, the basic capacity for infectious disease surveillance is lacking (Hinton 2001). Time lags, communications difficulties, and personnel shortages render the system unable to respond rapidly (Smithson and Levy 2000, 247). Thirteen states lack an epidemiologist, 18 percent of public health laboratory positions are vacant, and only 20 percent of local health departments have plans to deal with bioterrorism. Resources entering the public health system for modernization come largely from the federal level and are heavily targeted to bioterrorism. Fiscal difficulties are resulting in reduced support for core public health tasks (Smith 2003). In Colorado, the state cut all funds for local health departments as a result of the influx of federal bioterrorism money, leaving some departments with funds for bioterrorism experts but no bud-

get for routine public health activities (Eban 2002). Local jurisdictions that were trained and engaged in planning are having difficulty gaining involvement by hospitals and medical personnel in training and planning activities (Heinrich 2001a). These deficiencies were observed during the 1999 West Nile virus outbreak in New York, where a relatively small outbreak taxed the resources of the largest local, state, and federal public health departments (GAO 2000).

Hospitals, in the current cost-conscious environment, lack surge capacity to deal with an emergency. By the late 1990s, the patient load from a routine influenza season was overtaking primary care and emergency departments (Richards et al. 2000; Derlet, Richards, and Kravitz 2001). Anecdotal evidence indicates that some hospitals actively avoid becoming involved in public health crises and discourage personnel from smallpox vaccination (Lurie 2002). Wetter, Daniell, and Tresser (2001), studying hospital emergency departments, found that less than 20 percent had done any planning for bioterrorism or other public health crises.

Although federal officials claim the bioterrorism initiative can assemble disaster medical assistance teams and drugs from the national pharmaceutical stockpile on-site within 12–24 hours, the best estimates are that, in reality, this would not occur for 48–72 hours (Heinrich 2001b). There would then be additional delays in utilizing the aid for treatment. The multiagency response mechanism diverts resources from front-line responders such as hospitals to centralized teams, at the cost of preparedness for those responders. Preparedness based on the security/law enforcement/natural disaster model disproportionately emphasizes the “siren” responders relative to the hospital and surveillance components, which are more likely to detect and deal with an infectious disease threat. National Guard RAID response teams, for example, cost enough to equip nearly 50,000 hospitals with decontamination facilities. Funds might be better spent to extend the shelf-life of local medical and drug supplies and to ensure local “bubble” programs. (Smithson and Levy 2000, 261–62, 296–98; Cohen 2000).

A large part of the blame can be placed on the patchwork manner in which preparedness policy has been developed and implemented, which is largely due to the direction of the policy stream. Drexler (2002, 267–68) notes that defining the problem as counterterrorism rather than as public health forces public health preparedness advocates to compete in the national security arena, and these frustrations have led to a game of “budget brinkmanship” between competing actors rather than a reasoned analysis of the problem and potential solutions. As a result, less than 1 percent of the \$9.7 billion terrorism budget in FY2001 went toward public health infrastructure. While

entrepreneurs have been successful in spurring action, the mismatch between the problem and solution have resulted in most new resources going to unintended uses. As epidemiologist Michael Osterholm (2000, 175–76), a prominent advocate of preparedness programs, notes, most of the funded projects for bioterrorism preparedness would actually play no role in a real incident.

The current federal bioterrorism program attempts to address some of these problems. Significant funding is provided for laboratory upgrades, surveillance, planning, and communications between state, local, and federal health authorities. This is all targeted, however, at terrorist incidents involving traditional military biological weapons. CDC training for laboratory staff, for example, focuses on diagnostics only for the targeted agents. Similarly, the focus on targeted agents means that few of the resources devoted to the program will address immediate, nonbiological warfare problems such as antibiotic resistance. The danger exists that these improvements will be compartmentalized and will not be applied to broader risks of epidemic disease.

In contrast, it is argued that the best tool for controlling public health threats is a broad-based program to improve the disease surveillance system (Foreman 1994, 146–49). Because addressing a problem requires first recognizing that it exists, this is an essential step toward improving the public health system. Unless we assume that all bioterrorism events will occur using agents on the priority list or will involve advance warning (contrary to the historical case), this is also the essential first step in identifying and responding to bioterrorism. In the current environment, this is being neglected. For example, despite the rapid increase in bioterrorism funding, funds for upgrading surveillance have remained flat (Zwilich 2003).

Foreman (1994, 147–49) argues that the need for contingency funding—that is, nontargeted funds to be used to address emergent problems based on the circumstances of the specific public health problem. In the case of the AIDS epidemic, funding would have created the type of flexibility envisioned by the emerging infections program—the ability to adapt to a new public health program—potentially limiting the scope of the American epidemic and saving thousands of lives.

Serious questions remain over whether categorical programs such as the bioterrorism program, even when based on sound public health practice, are the best approach to dealing with public health problems. In the 1990s, the Public Health Practice Program Office at the CDC raised “concerns that categorical programs limit flexibility and elasticity within the public health system, resulting in sub-optimal performance when assets are redeployed in response to emergencies” (Turnock and Atchison 2002, 74). Furthermore, the use of the rhetoric of bioterrorism to gain

public health resources has the potential to create new problems in the form of hysteria and hoaxes. More than 200 hoaxes were logged between 1997 and 1998, of which 13 involved more than 200 potential victims. These were blamed on the effects of media coverage and the rhetoric of government officials (Cole 1999). Each involved significant opportunity costs to the individuals and agencies involved. Panic over the availability of the antibiotic ciprofloxacin during 2002 led the federal Department of Health and Human Services to threaten to abrogate the manufacturer’s patent rights in order to obtain a lower price, creating new barriers to the development of new vaccines and treatments (Calfee 2001).

In summary, a need exists to upgrade the American public health system. Both programs under consideration do this, but the current bioterrorism initiative does so by targeting specific agents that may not be effective in dealing with nonbioterrorist public health problems, and that may in fact aggravate the problem of bioterrorism hoaxes.

What Is the Solution?

Richards, O’Brien, and Rathbun (2002, 72) suggest that “[t]he best way to manage the risk of bioterrorism is not to expend precious resources and political credibility on low frequency events, such as bioterrorism, but to focus on day to day public health functions, i.e. channel public and legislative fears about bioterrorism to fears about everyday public health.”

The basic needs of bioterrorism preparedness remain the basic tasks of public health—identifying unusual disease events, their cause, and intervening to alleviate the situation. The CDC recognized this in 1998 in its original proposal for rebuilding the infectious disease infrastructure, in which plans for building surge capacity for unusual and complex events—including but not limited to bioterrorism—was an integral part. At its core, this proposal included strategies to improve surveillance and response, research, infrastructure and training, and prevention and control measures. Ultimately, the rush to minimize the consequences of a potential bioterrorism attack shifted this broad-based reform of the public health infrastructure to a narrowly focused, resource-rich, and flawed program.

The general approach offers a number of significant advantages. For example, broad-based surveillance improvements can improve the identification not only of disease events involving feared weaponized diseases, but also other unusual disease events, such as the 1999 introduction of West Nile fever into the United States. A system that improves the ability to identify any disease event automatically improves the ability to identify man-made disease events, while the reverse is not necessarily true. It is easier to evaluate the effectiveness of the surveillance sys-

tem because a higher frequency of use creates more opportunities to detect and correct flaws. Upgrading public health laboratory equipment for broad-based surveillance avoids the threat of tunnel vision that is inherent in the bioterrorism-specific approach. In some cases, coordination with non-public-health agencies can produce useful public health surveillance tools, such as the 2000 CIA national intelligence estimate on global infectious disease (Gordon, Noah, and Fidas 2000).

Research is needed to develop cost-effective means to establish local health care surge capacity and larger pharmaceutical reserves at the local level, not just for bioterrorist attacks, but also for dealing with natural epidemics. It is not realistic to expect the current stockpile system to respond within 12 hours. Certain models, such as local emergency agencies developing banks of common antibiotics and other drugs, allow this to be done at a relatively low cost. Even a relatively small increase in local reserves and hospital resources can buy an additional 12–24 hours for federal emergency assistance to arrive in a crisis. While national stockpiles may be useful in a large-scale event, they may not be needed in a small, higher-probability incident and are not immediately available when a crisis is identified.

Because infectious disease threats arise at the local level and because of resource distributions, they must be responded to at the local level, and the emphasis in preparedness needs to be on improving infrastructure at the state and local levels. Lipsky (1971) and Hjern (1982) suggest that successful policy implementation requires attention to the street-level operators and their active participation in planning and development. Centralized control—in this instance, an artifact of the national security ethos of anti-terrorism policy—is an example of what is described as a system in which, “By consistently taking the power to make decisions about the ways to innovate, adapt, and coordinate efforts away from those who are directly affected, policymakers have created institutions that are less able to respond to the problems they were created to address” (Ostrom 2000, 33).

Thus, a successful program must ensure that trained personnel are available at the local and state levels, that communication between local, state, and federal public health agencies is adequate, and that planning and coordination with local and state emergency responders and health care workers occurs. Integration of and cooperation with local health care providers will be far easier if the training and planning that occurs is more relevant to the day-to-day tasks of the responders. For example, the failure to obtain cooperation by health care workers in the voluntary smallpox vaccination program has been blamed on the failure to involve local health care leaders in the planning process (*Washington Post* 2003). A strong start has been made

on the communications issue within the bioterrorism program; however, this would have occurred under the original infrastructure-building plan as well. Legal reforms need to be sensitive to the local political environment, local values, and the situation-specific needs of a public health emergency. Rather than seeking broad powers with wide impact in order to distribute the burden of an emergency, the focus should be on responding in a way that addresses the problem with minimum impact on civil and property rights. Distributive justice is better served by broad protections than by broad burdens.

AIDS, SARS, drug-resistant tuberculosis, hantavirus, West Nile fever—all offer clear and recent evidence that infectious disease remains a serious threat to population health, and that the public health system needs more attention than it has received. Preparing for these threats, however, requires appropriate policies to be in place for dealing with them. Rather than taking the easy path of developing bioterrorism-specific plans that are popular but must compete in the political environment dominated by interests, reframing the problem as a problem of public health would allow agencies to use the policy window created by public apprehension to generate public—and hence political—support for broader public health concerns. Policy windows exist for a finite period, and entrepreneurs must be ready to take advantage of them with alternatives that meet their goals, as well as answer and define the nature of the problem creating the window. Once the problem has been defined, the definition highlights some policy options and others fade in importance (Kingdon 1984). As Richards, O’Brien, and Rathbun (2002) note, police, firefighters, military, and other agencies competing for a role and resources in the current political environment are visible and have strong, active lobbies, an advantage in the competition for resources in the public health sector. Defining the terms of the competition as traditional public health problems would avoid the mistakes of the past and better serve the public interest in protecting public health, both from the threat of bioterrorism and naturally occurring disease. The United States is in urgent need of improvements to ensure that its public health infrastructure is able to meet threats such as emergent diseases, diseases evolving to resist treatment, and epidemics created out of human spite. While the current antibioterrorism approach may address some of the latter threats, a less targeted improvement plan is a sounder approach to the larger issue.

References

- Alibek, Ken, and Stephen Handelman. 1999. *Biohazard*. New York: Random House.
- Anderson, James H. 1998. *Microbes and Mass Casualties: Defending America against Bioterrorism*. Backgrounder 1182. Washington, DC: Heritage Foundation.
- Annas, George G. 2002. Perspective: Bioterrorism, Public Health, and Human Rights: Taking Human Rights Seriously Is Our Best Defense against Terrorism and Fosters Both Federalization and Globalization of Public Health. *Health Affairs* 21(6): 94–97.
- Ashford, David A., Robyn M. Kaiser, Michael E. Bales, et al. 2003. Planning against Biological Terrorism: Lessons from Outbreak Investigations. *Emerging Infectious Diseases* 9(5): 515–19.
- Berkelman, Ruth L., and Jim H. Hughes. 1993. The Conquest of Infectious Diseases: Who Are We Kidding? *Annals of Internal Medicine* 119: 426–28.
- Berkelman, Ruth L., Ralph T. Bryan, Michael T. Osterholm, James W. LeDuc, and Jim M. Hughes. 1994. Infectious Disease Surveillance: A Crumbling Foundation. *Science* 264(5157): 368–70.
- Block, Steven M. 2001. The Growing Threat of Biological Weapons. *American Scientist* 89(1): 28.
- Brownlee, Shannon. 2001. Under Control—Why America Isn't Ready for Bioterrorism? *New Republic*, October 29, 22.
- Bryan, Jacqueline L., and Helen Fox Fields. 1999. An Ounce of Prevention Is Worth a Pound of Cure—Shoring Up the Public Health Infrastructure to Respond to Bioterrorist Attacks. *American Journal of Infection Control* 27(6): 465–67.
- Calfee, John E. 2001. *Bioterrorism and Pharmaceuticals: The Influence of Secretary Thompson's Cipro Negotiations*. AEI Papers and Studies, November 1. Washington, DC: American Enterprise Institute.
- Calvert, Randal. 1985. The Value of Biased Information. *The Journal of Politics* 47(2): 530–55.
- Center for Civilian Biodefense Studies. 1999. CDC Releases Close to \$41 Million for Biodefense. *Biodefense Quarterly* 1(2): 1–2.
- . 2000. DHHS FY2000 Anti-terrorism Funding. *Biodefense Quarterly* 1(4): 4.
- Centers for Disease Control and Prevention (CDC). 1998. *Preventing Emerging Infections: A Strategy for the 21st Century*. Atlanta: CDC.
- Choo, Kristin. 1999. A Plague in the Making: U.S. Lacks Legal Structure to Fight Bioterrorism, Critics Say. *American Bar Association Journal* 85(12): 18.
- Cohen, L.P. 2000. Safe and Effective: Many Medicines Remain Potent for Years Past Their Expiration Dates. *Wall Street Journal*, March 28, A1.
- Cole, Leonard A. 1999. Risks of Publicity about Bioterrorism: Anthrax Hoaxes and Hype. *American Journal of Infection Control* 27(6): 470–73.
- Committee for the Study of the Future of Public Health. 1988. *The Future of Public Health*. Washington, DC: National Academy Press.
- Cosmides, Leda, and John Tooby. 1994. Better than Rational: Evolutionary Psychology and the Invisible Hand. *American Economic Review* 84(2): 327–32.
- Dalton, Patricia A. 2002. *Combating Terrorism: Intergovernmental Cooperation in the Development of a National Strategy to Enhance State and Local Preparedness*. Washington, DC: General Accounting Office. GAO-02-550T.
- deLeon, Peter, and Linda deLeon. 2002. What Ever Happened to Policy Implementation? An Alternative Approach. *Journal of Public Administration Research and Theory* 12(4): 467–92.
- Derlet, Robert W., John R. Richards, and Richard L. Kravitz. 2001. Frequent Overcrowding in U.S. Emergency Departments. *Academic Emergency Medicine* 8(2): 151–55.
- Deqn, P.K., A.M. Fry, K. Laserson, et al. 2002. Inhalational Anthrax Outbreak among Postal Workers, Washington, DC: 2001. *Emerging Infectious Diseases* 8(10): 1066–72.
- Drexler, Madeline. 2002. *Secret Agents: The Menace of Emerging Infections*. Washington, DC: Joseph Henry Press.
- Eads, George C., and Michael Fix. 1984. *Relief or Reform: Reagan's Regulatory Dilemma*. Washington, DC: Urban Institute.
- Eban, Katherine. 2002. Waiting for Bioterror: Is Our Public Health System Ready? *The Nation* 275(20): 11.
- Etzioni, Amitai. 2002. Public Health Law: A Communitarian Perspective. *Health Affairs* 21(6): 102–4.
- Falkenrath, Richard A., Robert D. Newman, and Bradley A. Thayer. 1998. *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack*. Cambridge, MA: MIT Press.
- Fee, Elizabeth, and Theodore M. Brown. 2001. Preemptive Biopreparedness: Can We Learn Anything from History? *American Journal of Public Health* 91(5): 721–26.
- . 2002. The Unfulfilled Promise of Public Health: Déjà Vu All Over Again: We Have Not Learned the Lessons of our Public Health History. *Health Affairs* 21(6): 31–43.
- Foreman, Christopher H. 1994. *Plagues, Products, and Politics: Emergent Public Health Hazards and National Policymaking*. Washington, DC: Brookings Institution.
- Garrett, Laurie. 2000. *Betrayal of Trust: The Collapse of Global Public Health*. New York: Hyperios.
- Geiger, H. Jack. 2001. Terrorism, Biological Weapons, and Bonanzas: Assessing the Real Threat to Public Health. *American Journal of Public Health* 91(5): 708–9.
- Gordon, D.F., D. Noah, and G. Fidas. 2000. *The Global Infectious Disease Threat and Its Implications for the United States*. National Intelligence Estimate 99-17D. Langley, VA: Central Intelligence Agency.

- Gostin, Lawrence O., Jason W. Sapsin, Stephen P. Teret, et al. 2002. The Model State Emergency Health Powers Act: Planning for and Response to Bioterrorism and Naturally Occurring Infections. *Journal of the American Medical Association* 288(5): 622–28.
- Hamburg, Margaret. 1999. Testimony before the Senate Appropriations Committee. 106th Cong., 1st sess., March 16.
- Heinrich, Janet. 2001a. *Bioterrorism: Review of Public Health Preparedness Programs*. Washington, DC: General Accounting Office. GAO-02-149T.
- . 2001b. *Bioterrorism: Public Health and Medical Preparedness*. Washington, DC: General Accounting Office. GAO-02-141T.
- Henderson, David A. 1993. Surveillance Systems and Intergovernmental Cooperation. In *Emerging Viruses*, edited by S.A. Morse, 283–89. Oxford, UK: Oxford University Press.
- Henretig, Fred. 2001. Biological and Chemical Terrorism Defense: A View from the “Front Lines” of Public Health. *American Journal of Public Health* 91(5): 718–19.
- Hinton, Henry L. 2001. *Combating Terrorism: Considerations for Investing Resources in Chemical and Biological Preparedness*. Washington, DC: General Accounting Office. GAO-02-162T.
- Hjern, Benny. 1982. Implementation Research: The Link Gone Missing. *Journal of Public Policy* 2(3): 301–8.
- Jernigan, David B., Pratima L. Raghunathan, Beth P. Bell, et al. 2002. Investigation of Bioterrorism-Related Anthrax, United States, 2001: Epidemiologic Findings. *Emerging Infectious Diseases* 8(10): 1019–28.
- Johnson, L.K. 2000. *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security*. New York: New York University Press.
- Katz, R. 2002. Public Health Preparedness: The Best Defense against Biological Weapons. *Washington Quarterly* 25(3): 69.
- Kauffman, Arnold F., Martin I. Meltzer, and George P. Schmid. 1997. The Economic Impact of a Bioterrorist Attack: Are Prevention and Postattack Intervention Programs Justifiable? *Emerging Infectious Diseases* 3(2): 83–94.
- Kayyem, Juliette. 2001. *U.S. Preparations for Biological Terrorism: Legal Limitations and the Need for National Planning*. BCSIA Discussion Paper 2001-4. Cambridge, MA: Harvard University, John F. Kennedy School of Government.
- Kincaid, John, and Richard L. Cole. 2002. Issues of Federalism in Response to Terror. *Public Administration Review* 62(Special Issue): 181–92.
- Kingdon, John W. 1984. *Agendas, Alternatives, and Public Policies*. 1st ed. New York: HarperCollins Publishers.
- Knott, Jack H., and Gary J. Miller. 1987. *Reforming Bureaucracy: The Politics of Institutional Choice*. Englewood Cliffs, NJ: Prentice Hall.
- Lederberg, Joshua, ed. 1992. *Microbial Threats to Health in the United States*. Washington, DC: National Academy Press.
- Lillibridge, Scott R., April J. Bell, and Richard S. Roman. 1999. Centers for Disease Control and Prevention Bioterrorism Preparedness and Response. *American Journal of Infection Control* 27(6): 463–64.
- Lipsky, Michael. 1971. Street-Level Bureaucracy and the Analysis of Urban Reform. *Urban Affairs Quarterly* 6(4): 391–409.
- Lurie, Nicole. 2002. The Public Health Infrastructure: Rebuild or Redesign? *Health Affairs* 21(6): 28–30.
- McCann, S. Anthony. 1999. View from the Hill: Congressional Efforts to Address Bioterrorism. *Emerging Infectious Diseases* 5(4): 496.
- McDade, Joseph E. 1999. Addressing the Potential Threat of Bioterrorism—Value Added to an Improved Public Health Infrastructure. *Emerging Infectious Diseases* 5(4): 591–92.
- McKinney, S. 2000. Testimony before the House Transportation and Infrastructure Committee, Subcommittee on Oversight, Investigations, and Emergency Management. 106th Cong., 2nd sess., May 4.
- Moynihan, Daniel Patrick. 1998. *Secrecy*. New Haven, CT: Yale University Press.
- National Commission on Terrorism. 2000. *Countering the Changing Threat of International Terrorism*. Report of the National Commission on Terrorism. <http://www.fas.org/irp/threat/commission.html>.
- Osterholm, Michael T. 1999. Bioterrorism: Media Hype or Real Potential Nightmare? *American Journal of Infection Control* 27(6): 461–62.
- . 2000. Emerging Infections—Another Warning. *New England Journal of Medicine* 342(17): 1280–81.
- Ostrom, Elinor. 2000. The Danger of Self-Evident Truths. *PS: Political Science and Politics* 33(1): 33.
- Pentland, Brian T., and Henry H. Rueter. 1994. Organizational Routines as Grammars of Action. *Administrative Science Quarterly* 39(3): 484–510.
- Pressman, Jeffrey L., and Aaron B. Wildavsky. 1973. *Implementation*. Berkeley: University of California Press.
- Richards, Edward P., Terry O'Brien, and Katharine C. Rathbun. 2002. Bioterrorism and the Use of Fear in Public Health. *Urban Lawyer* 35(3): 685–726.
- Richards, John R., Misty L. Navarro, Robert W. Derlet, and A. Antoine Kazzi. 2000. Survey of Directors of Emergency Departments in California on Overcrowding. *Western Journal of Medicine* 172(6): 385–88.
- Roman, Peter J. 2002. The Dark Winter of Bioterrorism. *Orbis* 46(3): 469–82.
- Roseneau, M.J. 1910. The Uses of Fear in Preventive Medicine. *Boston Medical and Surgical Journal* 162(10): 305–7.
- Rosenau, William. 2001. Aum Shinrikyo's Biological Weapons Program: Why Did It Fail? *Studies in Conflict and Terrorism* 24(4): 289–301.
- Sidel, Victor W., Hillel W. Cohen, and Robert M. Gould. 2001. Good Intentions and the Road to Bioterrorism Preparedness. *American Journal of Public Health* 91(5): 716–17.
- Siegel, Marc. 2002. The Anthrax Fumble: Bureaucratic Timidity and Turf Battles Needlessly Put Many Americans at Risk. *The Nation* 274(10): 14.
- Siegrist, David W. 1999. The Threat of Biological Attack: Why Concern Now? *Emerging Infectious Diseases* 5(4): 505–8.
- Smith, Stephen. 2003. Anthrax vs. the Flu. *Boston Globe*, July 29, C1.

- Smithson, Amy E., and Leslie-Anne Levy. 2000. *Ataxia: The Chemical and Biological Terrorism Threat and the U.S. Response*. Report 35. Washington, DC: Henry L. Stimson Center.
- 't Hart, Paul, Uriel Rosenthal, and Alexander Kouzmin. 1993. Crisis Decision Making: The Centralization Thesis Revisited. *Administration and Society* 25(1): 12–45.
- Tobin, R.J. 1986. New Federalism and State Implementation of the Clean Water Act. Paper presented at the Annual Meeting of the Southwest Political Science Association, March 19–22, San Antonio, TX.
- Torok, T.J., R.V. Tauxe, R.P. Wise, et al. 1997. A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars. *Journal of the American Medical Association* 278(5): 389–95.
- Travis, Rick, and Nikolaos Zahariadis. 2002. A Multiple Streams Model of U.S. Foreign Aid Policy. *Policy Studies Journal* 30(4): 495–514.
- Treadwell, Tracee A., Denise Koo, Kathleen Kuker, and Ali S. Khan. 2003. Epidemiologic Clues to Bioterrorism. *Public Health Reports* 118(2): 92–98.
- Tucker, Jonathon B. 1999. Historical Trends Related to Bioterrorism: An Empirical Analysis. *Emerging Infectious Diseases* 5(4): 498–504.
- Turnock, Bernard J., and Christopher Atchison. 2002. Governmental Public Health in the United States: The Implications of Federalism. *Health Affairs* 21(6): 68–78.
- U.S. General Accounting Office (GAO). 1999. *Combating Terrorism, Opportunities to Improve Domestic Preparedness Program Focus and Efficiency*. Washington, DC: General Accounting Office. GAO/NSIAD-99-3.
- . 2000. *West Nile Virus Outbreak: Lessons for Public Health Preparedness*. Washington, DC: General Accounting Office. GAO/HEHS-00-180.
- Walsh, E., and J. Mintz. 2003. Huge Homeland Security Drill Planned. *Washington Post*, May 5, A09.
- Washington Post*. 2003. Smallpox Fiasco. July 14, A20.
- Waugh, William L., Jr., and Richard T. Sylvester. 2002. Organizing the War on Terror. *Public Administration Review* 62(Special Issue): 145–53.
- Wetter, Donald C., William Edward Daniell, and Charles David Tresser. 2001. Hospital Preparedness for Victims of Chemical or Biological Terrorism. *American Journal of Public Health* 91(5): 710–16.
- Wildavsky, Aaron B. 1988. *Searching for Safety*. New Brunswick, NJ: Transaction Publishers.
- Wilson, James Q. 1989. *Bureaucracy: What Government Agencies Do and Why They Do It*. New York: Basic Books.
- Wise, Charles R., and Rania Nader. 2002. Organizing the Federal System for Homeland Security: Problems, Issues, and Dilemmas. *Public Administration Review* 62(Special Issue): 44–58.
- Zwilich, T. 2003. Lawmakers Urge Bioterror, Disease Surveillance Law. *Reuters*, May 5.