CENTER FOR TECHNOLOGY AND
NATIONAL SECURITY POLICY

Catastrophic Bioterrorism—What Is To Be Done?

by Richard Danzig

August 2003

Catastrophic Bioterrorism—What Is To Be Done?

by Richard Danzig

AUGUST 2003

CENTER FOR TECHNOLOGY AND NATIONAL SECURITY POLICY
NATIONAL DEFENSE UNIVERSITY
WASHINGTON, D.C.

The Center for Technology and National Security Policy

The Center for Technology and National Security Policy was established in 2001 to analyze national security issues that are significantly affected by technology. Its staff composition is designed to create synergy between senior scientists and defense policy analysts. The Center provides private advice to the Department of Defense, publishes articles, and hosts conferences. Its major programs include: military transformation, information technology, defense science and technology, biological sciences, social science modeling, and curriculum support.

Research and writing for this paper were completed in June 2003.

Contents

Introduction

It is now widely recognized that terrorists may inflict great trauma upon us by using biological weapons (bacteria, viruses, or toxins[1]) against America's civilian populations. There is, however, no common perception of how this problem should be defined and countered. In the language of today's business consultants, neither the "problem space" nor "the solution space" has been well mapped. In military terms, we do not have an "operational concept." In common sense terms, we have not established a method of focusing our efforts, testing alternative strategies, setting requirements, and determining priorities.

This paper is designed to show how we can do these things. It is organized in five major sections.

The first section shows why bioterrorism demands extraordinary preparation.

The second develops the argument that current preparation is flawed by the absence of a common, systemic, operational understanding of bioterrorist threats. Though different aspects of the problem (for example, the ability to weaponize certain agents, the value of vaccines, the potential contributions of detectors, or requirements for hospital beds) are at least partially understood, the whole is not linked into a unified concept of operations. Our agencies operate now like independent fingers, each poking at a problem, while the hand is unable to grasp the task in totality.[2]

The third proposes that we coordinate our efforts by establishing a set of common planning cases. It recommends that, in the near term, we focus on four particular cases to guide Federal agencies in their preparations for bioterrorism directed against our civilian populations.[3] (In the course of the paper, 12 particularly salient recommendations are advanced.) It also shows how to counterbalance the difficulties that come with this approach by, among other things, establishing a "case 5 committee."

The fourth section begins the recommended effort of analyzing cases and capabilities. It does this by focusing closely, in two of the cases, on two kinds of capabilities that are important to our biodefense. This analysis yields concrete—and in my judgment, imperative—recommendations for countering these threats. Most significantly, this discussion is an illustration of the rewards of the method I am proposing.

The fifth section identifies 10 capabilities that we must improve if we are to successfully counter bioterrorism. It is a map of the contexts in which I believe we should apply the techniques illustrated in the preceding section. A broad and fruitful planning effort will, I believe, evolve from assessing these capabilities in the context of selected cases.

I will participate in this broad effort, but seek by the publication of this document to engage others in this work, whether in their own organizations, with one another across organizations, or in collaboration with me.

Section 1

Why Bioterrorism Warrants Exceptional Preparation

A number of studies have identified American vulnerabilities to terrorism. Around the globe, terrorists have attacked airplanes, ships, trains, buses, office buildings, embassies, markets, theaters, resorts, monuments, government officials, businesspeople, and individuals who simply happened to be in the wrong place at the wrong time. Rarely have such attacks involved biological weapons.[4] Why then do these weapons warrant extraordinary attention?

Many have observed that biological weapons are "a poor man's atomic bomb." A single biological attack can kill a great many people, while the technologies to develop and deliver these weapons are relatively inexpensive, accessible, and difficult to detect, much less interdict. However, an additional attribute of bioterrorism would, if commonly recognized, amplify these concerns. I call this phenomenon "reload." To understand it, contrast the 9/11 air hijacking attacks with the anthrax letters that followed in the fall of 2001 and even more pointedly with the outdoor (aerosol) biological attacks that could occur in the future.

After inflicting a national trauma on 9/11, the attackers could not promptly repeat their achievement. They had consumed resources that were difficult to replenish (trained pilots willing to sacrifice themselves). Even more significantly, the modality that they used depended, in some measure, on surprise. Once alerted to this technique, we had some ability to counter it. Passengers on the fourth 9/11 aircraft fought back. (Months later, passengers and crew similarly overpowered a terrorist attempting to set off a bomb concealed in his shoe.) National authorities could (and did) ground airliners. Later, we flew fighter aircraft over our cities. In the longer term, we took security measures that significantly impede hijacking. As a result, any further attacks of this magnitude will probably need to employ different weapons in a different manner.

When the anthrax letters were mailed, 11 people contracted inhalational anthrax, 5 of whom died. Call this "5/11."Although the number of casualties was limited, the national security vulnerabilities made apparent by 5/11 are greater than those associated with 9/11. This is because of reload. Attackers who use biological weapons probably can avoid prompt detection and stockpile or replenish resources that permit repeated attack. Making a gram of readily aerosolized anthrax spores in a weaponized 1-to-5-micron range is a technical challenge, but, once production is accomplished, it is a much lesser challenge to make 1 kilogram. And it is not a significant challenge for a terrorist organization that can make a kilogram to make 10 or 100 kilograms.[5] Nor, absent exceptional luck, do we have effective means of interdicting a biological attack, even if we know that one has already occurred and that others are on the way.[6] This is especially true with respect to outdoor (aerosol) attacks. While we can shut down our mail system (with great economic consequence—think how taxes and bills are paid and parcels are shipped), we cannot shut down the atmosphere.

The gram of anthrax mailed to Senator Patrick Leahy reportedly contained one trillion spores of anthrax. Since inhalation of 8,000 to 10,000 spores is generally regarded as likely to be lethal for the average

person,[7] a gram perfectly effectively and efficiently disseminated outdoors under optimum weather conditions and inhaled by an unprotected population theoretically could kill 100,000 people. Outdoor dissemination in liquid or powder form would not be difficult. Of course, a perfectly efficient distribution and exposure rate would not be achieved. All calculations of infection and lethality associated with biological weapons are uncertain,[8] but a reasonable approximate planning premise is that a gram of anthrax released in an urban area might expose between 100 and 1,000 people to a lethal dose. A kilogram (containing 1,000 trillion spores) could be anticipated to infect tens of thousands of people.

The ability to reload and repeat an attack obviously amplifies the number of potential victims. An attacker, having disseminated anthrax one evening in Washington, for instance, could do the same thing the next day in Detroit, Chicago, or Los Angeles.[9] We are very unlikely to observe the act of attack. A terrorist can surreptitiously disseminate anthrax from any of an immense number of points upwind from a target. Even if detectors (a scarce resource) are in position and operating, reporting, and being instantly monitored, an attack is unlikely to be evident for many minutes, and its source will probably not be pinpointed for hours (if ever). If detectors are not available, an attack will probably not be evident until the first patients appear in large numbers at emergency rooms, more than 24 hours later. During this time, an attacker can readily move to another site, with a prepositioned (or very portable) stockpile of anthrax.

In sum, biological weapons readily lend themselves not only to catastrophic effects but also to reload. This is a special attribute. Even a terrorist detonation of a nuclear weapon, catastrophic as it would be, is not likely to be repeated quickly.

Campaign Terrorism

Reload is especially important in the context of political terrorism. Some terrorism is expressive. A nihilist, vandal, or lunatic who believes he is initiating an apocalypse may see his act as an end unto itself, a self-contained assertion of his or his god's anger or power. The terrorists of most concern to us act, however, for instrumental reasons. They produce terror as a means to a political end.

Acts of terror may achieve political ends by physical destruction, but they operate primarily in psychological and political dimensions. Instrumental terrorists aim to disable governments by diverting resources, enhancing divisiveness, and undermining the confidence of citizens in their government. Ultimately, if a government cannot protect its citizens, acts of terror sap their targets' will to persevere in policies the terrorists oppose. Viewed this way, terrorists and governments may be thought of as in a competition over whether the safety and morale of the target population can be maintained.

Reload is of enormous importance in this context. Traditional acts of terrorism enjoy climaxes but exhaust themselves and then face the prospect of retaliation. Biological terrorism affords the possibility of repeated attack, undermining confidence and forcing ever-escalating investments of resources to achieve a modicum of defense. If, during a period of recurring biological attack, we are inadequately prepared, then the psychologically and politically corrosive consequences of the attack will be amplified, as our population will ask: why wasn't more done? In the extreme but chillingly plausible case, an unprecedented effect may be achieved: our national power to manage the consequences of repeated biological attacks could be exhausted while the terrorist ability to reload remains intact.[10]

This paper is designed to suggest how we can better prepare for such attacks. A first step is to recognize the risk of reload and to prepare accordingly. One of the most important questions military commanders are trained to ask when they are under fire is: "Is this the first in a series of attacks?" The answer, gleaned from intelligence, guides the commander's force posture, tactics, and allocation of resources. We have slighted this question in our planning for bioterrorism.

Recommendation 1: Establish planning scenarios and set resource requirements on the assumption that biological weapons will permit terrorists to rapidly "reload" and repeatedly attack. In this light, we must prepare for biological attacks repeated in different American cities rather rapidly after one another. Plan to defend against a campaign, not just an attack.[11]

Section 2

The Absence of a Common, Systemic, Operational Understanding

Ordinarily, the response to a national security problem is debated and then resolved by participants who share a common understanding of a threat and of the capabilities relevant to addressing that threat. For example, those who command ships, those who design them, and those who are responsible for naval strategy and policy share an understanding of how ships may be exposed to attack. They also understand the operational capabilities and physical assets required for ship self-defense, including missile and aircraft intercept systems, methods of protection against other ships, the uses of protective armor, methods of evasion, techniques of damage control, etc. This understanding is no doubt imperfect, and there may be debate about whether and how, for example, to design a new class of ships or to conduct an operation. But the expert participants in these debates will typically benefit from a common vocabulary and training. Many will have fought with the types of weapons or forces in question, and all will have read about or talked with others who have. Though they may have different perspectives, all decisionmakers are using commonly understood tools in an integrated fashion to address a commonly comprehended problem. They have a common, systemic, operational understanding.

This is not the situation at present in grappling with the threat of bioterrorism. We have almost no experience with intentional biological attacks. For more than three decades we have not had an offensive program that might inform our defensive sensibilities.[12] Moreover, the bioterrorist threat is described as consisting of a confusing array of particular agents, each with different characteristics. Each of these agents may in turn be distributed in many different ways. Bewildered by these complexities, we have, in military terms, failed to develop a coherent "picture of the battlespace." This failure is then compounded by the fact that experts who must operate in this battlespace come from vastly different backgrounds and approach this cluster of problems with very different priorities, skills, resources, and perspectives. Microbiologists, epidemiologists, emergency physicians, hospital administrators, veterinarians, physicists (working on detector systems and dissemination models), Federal Bureau of Investigation analysts, military personnel, Federal Emergency Management Agency experts, city police officers, lawyers, infectious disease experts, intelligence analysts, executives at large pharmaceutical and start-up biotech companies, and a host of others bring greatly varying knowledge, intuitions, approaches, and perceptions of the problems they are trying to solve.

Without a common framework, when asked to address problems of bioterrorism each of these experts understandably emphasizes his or her preferred technology or approach and then employs it without meaningful reference to the requirements and opportunities developed by those with different expertise or perspectives. As a result, individual efforts do not relate to an overarching strategy, measures of success are difficult to devise, relevant tools are not seen as alternatives or complements to one another, and resources are allocated more in accord with bureaucratic position and power than in response to the problem.

The resulting incoherence is particularly debilitating for government bureaucracies. Friedrich Nietzsche observed that the most common form of stupidity is forgetting what one is trying to do.[13] This is certainly true of the bureaucracies that are inevitably the instruments of our response to bioterrorism. A bureaucracy operates effectively in direct proportion to the clarity of its marching orders. When components are left to choose their own planning premises, the predominant response is to relabel or at best slightly redirect ongoing activity. Scattered, then, in many different directions, our society has the equivalent of a nervous breakdown—it cannot coordinate its efforts.

Along with incoherence, we now also suffer from rigidity of thought. The threat of biological attacks upon our civilian populations is a new problem and must be thought about in a new way. Present methods of protecting our population are largely derived from techniques and tools developed to deal with two other circumstances: protecting the military against chemical attack and protecting civilians against natural outbreaks of disease. New opportunities—for example, using civilian air filter systems as means of protection or detection or dealing with more cases than hospitals can handle by developing systems of mobile or home care—are not given adequate attention. It is imperative that we find a framework that helps us to focus and forces us to think afresh.

Section 3

Creating a Common, Systemic, Operational Understanding: Four Cases for Planning

A straightforward approach to attacking this problem would first organize near-term responses to the threat of civilian bioterrorism around a minimal number of representative cases. With a suite of scenarios in mind, we can then identify categories of operational skills (detection, intelligence, consequence management, etc.) most relevant to countering the threat. We can then give content to these categories by identifying what these skills can contribute, how they must be developed, and how they may be coordinated and applied in each of these cases.

The cases, it must be emphasized, are only a means to an end. They provide an anvil against which to hammer out capabilities. It is the capabilities that are important. The contexts in which they will be applied cannot confidently be predicted. One common characteristic of 9/11 and 5/11 was that both surprised us.[14] We must therefore anticipate that we will again be surprised. But by constantly matching cases to our operational understanding, we will have a method of analysis that can catalyze and focus the evolution of capabilities that will be useable for a broad range of cases, some of them not even capable of being anticipated today.[15]

The choice of planning cases can always be debated, but I believe that a limited number can represent our most significant risks, illuminate how our systems would be taxed,[16] and stimulate a broad range of preparations. After discussion with a large number of senior policymakers and experts, I believe that a consensus can be created around four cases as our near term planning premises.[17] These are:

- Case 1: A large-scale outdoor aerosol anthrax attack
- Case 2: A large-scale outdoor aerosol smallpox attack[18]
- Case 3: An attack that disseminates botulinum toxin in cold drinks
- Case 4: An attack that spreads foot and mouth disease among cattle, sheep, and pigs.

As noted below, these cases are not the be-all and end-all of biological terrorism. Other agents and dissemination techniques can certainly be used. However, I will make three assertions, labeled strong, stronger, and strongest, about the cases I am recommending.

Strong Assertion. At a minimum, we must address these cases. They are real, possibly imminent, and very substantial dangers. Virtually all experts and policymakers agree with this. No program of biological defense can be considered adequate if it does not address these cases.

Stronger Assertion. Addressing these planning cases will have great collateral rewards for all cases. For example, the consequence management techniques (mass vaccination capabilities, emergency room procedures, and so forth) developed to deal with an outbreak of smallpox will be valuable in dealing with all other contagious diseases; an antibiotic stockpile developed for anthrax will help in countering many other susceptible bacterial agents.

Strongest Assertion. In the near term, these four planning cases are broadly representative of the great majority of cases that should concern us. Put another way, in the immediate future most attacks are likely to be versions, often lesser versions, of these cases. They may require some modification of the general approach and some particular applications, but as a general matter, if we can handle the planning cases, we are likely to be able to handle the other cases that most probably threaten us in the near term.[19] For instance,

plague is both a contagious disease, like smallpox, and a bacterium, like anthrax. If we can deal with the contagious aspects of smallpox and the treatment requirements for anthrax, we are likely to be able to deal with plague (which is far less contagious than smallpox and more responsive to treatment than anthrax). Plague will require specific detector and diagnostic capabilities and its own vaccine. But, as a general matter, plague is a lesser-included case. Similarly, smallpox could be spread by an infectious individual coughing in the faces of those with whom he had some extended contact, for example on a prolonged and crowded subway trip. But if we had planned for a large aerosol attack, those plans would stand us in good stead for the smaller problem, even if 100 or 200 infections were generated by person-to-person contact.

If adopted, the planning cases can be used in four different ways. First, an awareness of the cases can catalyze action—they make a diffuse threat more understandable, concrete, and real. Second, they can become a method of orchestrating our efforts; when used as premises for our planning, they establish a clear beat to which our bureaucracies can march. Third, they can serve as a template to assess our position, prioritize proposed investments, and measure progress. Finally and most importantly, the cases can serve as an anvil against which to hammer hypotheses, enabling us to establish requirements[20] and to test the validity of different strategies for dealing with catastrophic bioterrorism. Focusing on these cases will allow experts from diverse backgrounds jointly to develop a concept of operations—first to deal with these cases, then with bioterrorism generally.

Recommendation 2: Use four attack cases (aerosol anthrax, aerosol smallpox, botulinum in drinks, and foot and mouth disease) as the planning premises for near-term work on bioterrorism throughout the Federal Government. Build a portfolio of required capabilities from these cases; test hypotheses about improvements to our defenses by assessing their value in dealing with these cases; measure progress against these cases.

With the benefits of the case framework comes a liability. As with any organizing structure, the cases can become a source of rigidity. They should be our near term planning premises. However, just as the Cold War orchestrating paradigm of a Soviet invasion of Europe did not preclude work on collateral issues (for example, strengthening our submarine force) and "advanced projects," so collateral and advanced biodefense work will still be required (for example, on Ebola and other hemorrhagic viruses).

Basic research must always be broadly defined. This proposal must not limit the range of that research. Anthrax, smallpox, and botulism are examples of illnesses that are caused in humans by a bacterium, a virus, and a toxin; foot and mouth disease unleashes a virus against our agricultural economy. Basic research should focus not only on the idiosyncrasies of these particular pathogens but also on the common mechanisms by which bacteria, viruses, and toxins attack—and on their vulnerabilities to counterattack.[21]

Because we cannot predict the precise nature of biological attacks, whenever multivalent approaches are available, they should be preferred to narrowly targeted approaches. Most significantly, we must be sensitive to the fact that biology, and therefore the threat of bioterrorism, will evolve much more rapidly and with fewer intelligence indicators than the threat of Soviet invasion. Today's bacteria, viruses, and toxins may become less significant as agents of biological attack than prions,[22] bioregulators,[23] or other new pathogens.[24] As new threats evolve, we will need a mechanism to guide our intelligence collection and analysis, to register indications and warnings, and then, if warranted, to adapt the existing cases and develop new cases that should be the focus of our attention. Recommendation 3 addresses this.

Recommendation 3: Establish a "Case 5 Committee" of scientists from government, academia, and biotech and pharmaceutical companies, as well as intelligence officers. Direct the committee to review, at least semiannually, the evolution of biology and of terrorist individual, group and state capabilities and activities in this arena. Have the committee identify indicators and warnings of the evolution of new threats, recommend intelligence efforts to document the evolution of those threats, and change the cases as warranted over the years ahead.

Section 4

Some Initial Observations and Recommendations about Two Capabilities in the Context of the Anthrax and Smallpox Cases

I believe that 10 capabilities (which I will identify below) will be fundamental to our success or failure in countering bioterrorism. From amongst these, I have selected two to demonstrate how an interweaving of cases and capabilities can deepen our understanding of what we need to do. The illustrative capabilities are our abilities to (a) detect a biological attack through the use of sensors; and (b) neutralize or mitigate agents by the use of drugs and vaccines. In this section, I will undertake a close evaluation of the anthrax and smallpox cases[25] with respect to these two capabilities. Because the case approach is systemic (a reward is that it integrates our thinking), this inquiry naturally leads to some connected observations about our medical surveillance and consequence management systems.

The Anthrax Case[26]

Assumptions

This case assumes the covert aerosol dispersion of several kilograms of weaponized anthrax spores in the 1-to-5-micron range on an evening during conditions of weather inversion in a major urban area. The assumed method of dispersion is by a small commercial sprayer from a single point source (for example, from a building). A resulting anthrax cloud is assumed to produce infection with lethal doses, if untreated, for the average person at least 40 miles downwind. The fatality rate for those infected within this area is anticipated to be 90 percent if untreated. At least 200,000 people are expected to be infected within this area. Smaller numbers of infections and fatalities are assumed to occur up to 120 miles downwind. Among those infected, the 5 percent who first begin manifesting flu-like symptoms are expected to do so within 24 to 48 hours.

Observations and Recommendations

The Federal Management Role

In the wake of the 1995 dissemination of the chemical nerve agent sarin by the terrorist group Aum Shinrikyo in the Tokyo subway system, a national effort began to prepare American city and state first responders for attacks using weapons of mass destruction.[27] This approach, which intensified after 9/11, is logical, legally sound, and politically attractive. Logically, if an attack is made evident by a note or explosive device, local police, fire, and ambulance crews are likely to be the first on a scene. Thereafter, the burden of many attacks will be felt most strongly by local health systems. Legally, our system looks predominantly to municipal, county, and state entities as the authorities of first resort for handling criminal and health problems. Politically, programs that direct money to local authorities are popular with Members of Congress and their constituents.[28]

Consideration of the anthrax case, however, makes it evident that there is a critical Federal management role that overarches the important work at the local level. An anthrax aerosol attack that extended in its primary effects over 40 miles and had significant collateral effects 120 miles downwind would overlap several jurisdictions. If it occurred in Washington, DC, it would likely also envelop portions of Virginia, Maryland, and possibly West Virginia and Pennsylvania. If

in New York, it would extend to New Jersey or Connecticut or both, and perhaps to Pennsylvania. Transient citizens of many other states and foreign countries would inevitably be among the victims.

More fundamentally, because anthrax, like other biological weapons, can be readily reloaded, an attack in one area would immediately induce and require other jurisdictions across the Nation to go on alert and undertake preparations for a similar attack. In this situation, the Federal Government would be expected to provide not only guidance and assistance but also action and direction.

Federal preparation has taken account of this with respect to smallpox because it is a contagious disease, but the requirement applies to anthrax (and other, lesser, cases) as well. Vaccine supplies, antibiotic stockpiles, detector capabilities, decontamination equipment, and a host of other scarce resources would have to be allocated between competing jurisdictions, with all demanding them. Requirements for tracking down the attacker and for reassuring the public would inevitably fall predominantly on Federal agencies. Inconsistencies in policy and advice (for example, on the proper treatment of anthrax victims and on the standards for safety in the presence of anthrax) would sow confusion, dispute, and perhaps panic. Local restrictions on movement or decisions to evacuate could be counterproductive and divisive. Only the Federal Government could provide the required consistency.

The range of demands on the President and Cabinet would be immense. The skills required to meet these demands would be diverse and scarce. It is imperative, then, to prepare a team of Federal experts who can advise policymakers at the highest levels about consequence management responses to such a crisis. During the anthrax letters crisis in the fall of 2001, the rudiments of such a team were put together on an ad hoc basis in the Old Executive Office Building and during extended telephone conference calls. One could be assembled again in the wake of new attacks. It would be vastly more valuable, however, to prepare for such attacks by establishing a cohesive and carefully selected team now.

The risk of reload puts a great premium upon prior formation of this group, as it does upon all forms of preparation. Others have suggested that while we have a mental model of warfare rather like the one we use for our form of football, terrorists are playing football in the form in which the rest of the world has developed the sport. (We call their game soccer.) Our game presumes a line of scrimmage and a clear differentiation between offense and defense. Their game creates a more fluid contest without any such lines of demarcation. Unfortunately, biological weapons' ease of reload intensifies this contrast: it suggests that the soccer model of continuous action will apply. We cannot assume that we will have time to huddle between biological attacks. We cannot presume on the model of Pearl Harbor that we will have time to train and organize after a first attack.

Accordingly, we should move now to create and prepare a team of experts within and outside of government. Such a group might be called a Biological Emergency Advisory Team, or BEAT. Its members would retain their regular positions but would be available for emergencies via call-back and conference call mechanisms, as well as in face-to-face meetings. They would gather periodically to train, develop camaraderie, and build a sense of which team members were best positioned to perform which tasks. Training would also permit team members to identify measures that would better position us to deal with bioterrorism. Such an effort would not displace the roles of state responders but would transcend those roles and make them more meaningful.[29]

Such a team should have significant redundancy. This is necessary partly because some experts would not be available in a crisis. They might be out of the country, themselves ill[30] or injured, or too deeply involved in their locality to be available at the Federal level. Redundancy also is necessary because a bioterrorist crisis, particularly if reload occurs, is likely to be prolonged. As a result, for central advisors and decision-makers, reload is likely to lead to overload.[31] Fatigue will become a factor. British studies of their foot and mouth outbreak (which lasted from February to August of 2001) emphasize the costs of fatigue, as a small number of people tried to manage a long-term catastrophe as though it were a short-term crisis.[32] To combat this, the BEAT must be substantial (50–100 people) and robust.

A designated and trained Federal team will also help us by beginning to identify the information and communication system needs that are required to operate in a crisis. In the event of a biological attack, and especially in the wake of a series of such attacks, situational awareness will be a huge challenge. The National Security Council, Department of Defense, Department of Health and Human Services, Centers

for Disease Control, the FBI, and components of the new Department of Homeland Security all have some information and communication systems, but these are not well tailored to work together to cope with domestic biological terror attacks.

Recommendation 4: Develop a Federal biological emergency advisory team now. Train the team in the cases described below and use them to deepen insight into resources and strategies that will be helpful to cope with these cases. Support the team and senior decisionmakers with information and communication systems that integrate the assets of all relevant agencies.

The Vaccine, Antibiotic, "Third Response" Triad

Mass vaccination issues are not confined to smallpox or other contagious diseases. Reload suggests that even a single aerosol anthrax attack, for example, will initiate demands for mass vaccination against anthrax. Our stockpile of anthrax vaccine, however, is limited to only a few million doses, intended largely for military use. In the event of a major aerosol attack, it would be inadequate. Even the presently debated goal of 25 million doses for use in an emergency—which is a long way from achievement—is likely to be inadequate.[33]

This concern is amplified by another point. Anthrax scenarios should not be based solely on the assumption that our stockpiled antibiotics will treat the disease. Development of an antibiotic resistant strain of *B. anthracis* (the bacterium that causes anthrax) is quite easy.[34] Even at the high school level, biology students understand that an antibiotic resistant strain can be developed by growing a bacterium (anthrax is a widely available agent) in a culture that includes a diluted application of the antibiotic expected to be used in treatment.[35] Some organisms will thrive better than others, signaling antibiotic resistance. These can then be harvested, allowed to replicate (under optimized conditions, *B. anthracis* replicates itself by division every 30 minutes), and selected again for antibiotic resistance. After a readily achievable number of generations, the resulting strain will be resistant.[36]

Antibiotic resistance will not defeat a vaccine. But because the anthrax vaccine is now commonly judged not to confer immunity until 35 days after vaccination[37], all Americans (save those previously vaccinated) can, for more than a month, effectively be hostage to an attacker using a broadly resistant strain. Even a narrowly resistant strain could induce great difficulty by forcing reliance on inadequately stockpiled antibiotics.[38]

To deal with this and other likely future developments, we should give great priority both to strengthening the two pillars of our existing defenses—our vaccine and antibiotics programs—and to developing a third alternative as quickly as possible. This third response would involve drugs that attack anthrax in other ways and at other stages of its infectious cycle.

The vaccine arm of this triad can be greatly strengthened by:

- determining whether immunity can be achieved with the existing vaccine faster than in 35 days (there is some evidence to this effect)
- expanding the stockpile of existing vaccine (this also must be done for other reasons, noted below)
- giving the greatest priority to the development of a better vaccine.[39]

In the longer term, as the Defense Advanced Research Projects Agency (DARPA) and key actors in the Department of Health and Human Services have urged, anthrax could be "taken off the table" if an improved vaccine were attractive enough to be administered as a matter of course to the entire American population. Concomitantly, our antibiotic defenses can be strengthened by developing and testing new types of antibiotics, by managing our stockpile to maximize its diversity as well as size, and by possibly reserving some antibiotics (perhaps those with secondary characteristics that make them unattractive for normal use) for emergency use.

The third arm of this triad is now only in the research stage. Promising methods would unleash postexposure protectants such as enzymes (lysins) or bacteriophages (viruses) that attack bacteria[40] or by administering antitoxins.[41] *B. anthracis* causes disease by secreting toxins that effectively poison the host. While antibiotics and bacteriophage enzymes would interrupt or preempt this by eradicating the bacteria themselves, anti-toxins would disable or neutralize a poison once produced.[42] These alternative treatments could be invaluable if we confronted an attack with a strain that was broadly resistant to antibiotics,[43] or if we became aware of the disease too late to treat it only with antibiotics, or for those who suffered from so large a dose that it overwhelmed the protection conferred by a vaccine.[44] Those closest to the point of attack who, from a terrorist standpoint, may be particularly high value targets (the President and his staff, members of Congress, key members of the military, hospital personnel, and so forth) may warrant intensive

supplemental protection. These "third approaches" could perform this function.[45] These approaches should receive accelerated testing, evaluation, and, if warranted, licensing and production. Even if expensive and in limited supply they could beneficially complicate an attacker's strategy, just as the bomber–land missile–submarine triad complicated a would-be nuclear attacker's task.

Recommendation 5: Establish a goal of developing a triad of antibiotic, vaccine, and a third response (for example, lysins, bacteriophages, or antitoxins) to anthrax. Diversify the antibiotic stockpile as much as possible. Accelerate the development of a new anthrax vaccine. In the interim, expand stockpiles of the existing anthrax vaccine. Begin production of a chosen third response drug as soon as possible.

Detector Requirements

Thus far, this paper has noted two special attributes of biological weapons: their ease of reload and their high potency relative to their low cost and ease of acquisition. We must also account for a third special characteristic: biological weapons do not announce themselves at the moment of attack. If a target population is subjected to bullets, conventional bombs, chemical assaults, or nuclear explosions, we are aware of the attack at the moment of exposure. Biological weapons are insidious because they are likely to be invisible and delayed in their effects while multiplying silently and exponentially within mobile and susceptible populations.

This creates a problem: if we are to know at the time of an attack that biological weapons are being used against us, we must invest resources to develop rather novel detection technologies. At the same time, the problem gives rise to opportunities. For instance, if we can detect the use of a biological weapon before its effects are felt (or at least fully felt), we may be able to warn and disperse or protect the target population before it is exposed. This is commonly called "detect to warn."[46]

Detect to warn is a prime goal for our military, in which service members are often in compact and demarcated bases, have protective equipment at hand, and are trained to respond to commands in the wake of an alarm. However, the concept of detect to warn is elusive even in the military context and is now generally regarded as not achievable in the near term for civilian populations. Warning of this kind would have to occur within minutes or, for people in downwind areas, within a few hours. It would also have to be accompanied by some self-protective steps that are not now established.

On the other hand, many laboratories and programs are engaged in an effort to meet a less demanding but still rewarding goal: "detect to treat." This is an attempt to get ahead of the effects of the disease by sounding an alarm before symptoms manifest themselves and then rapidly treating those who have been attacked. The approach is promising because for many agents, including anthrax, prophylactic administration of antibiotics within the first few days (that is, typically before the onset of signs and symptoms) will save a large number of lives.

Unfortunately for those who fund and develop detectors, there is little clarity about what is required to achieve either civilian protection or efficacious advance notice of the need for treatment. In the absence of stated requirements, detector research and development is pushed by technology opportunity rather than pulled by demand for utility in real world circumstances. Using the four cases, a more concrete sense of demand can be created that would better orient and focus our investment decisions. We can see this by focusing on two variables that have posed particular difficulty for the detector community: false alarms and speed of alert.

False Alarms

Detection of an aerosol attack is a challenging technical problem. The air that we inhale contains millions of particles, including pollen, molds, fungi spores, and hundreds of species of bacteria (many of them uncataloged). It varies greatly according to season, weather (including microweather patterns around buildings, hills, and other obstacles), time of day, and the presence of human variables (vehicles, construction activities, pesticide spraying, fires, and so forth). An aerosolized biological weapon would be a small additional presence in this vast sea of variables. In technical terms, the signal-to-clutter ratio is very low. There is a substantial likelihood that the signal would be lost in the background clutter.

These difficulties manifest themselves, among other ways, in a significant error rate. We worry about the possibility that we may be attacked, but our detection systems will fail to sound an alarm. Our systems may not be sensitive to some agents, some normally detectable agents may be altered to render them undetectable, some agents may be infectious in quantities beneath detector sensitivities[47], the environment may

be so polluted that we cannot detect an agent, and our detectors may not be numerous or well positioned enough to detect an attack.

These problems are being addressed by the technical ingenuity of our national laboratories and contractors. They are, however, linked to a set of problems that are broader than technology alone can resolve. When an air sample is collected, particles within it differentiated, and those with suspect characteristics tested, the results disquietingly often suggest an attack when one has not in fact occurred. This is a "false positive" result. A significant false positive rate can be tolerable for disciplined military forces that are used to risk, accustomed to false alarms, and trained to protect themselves. It is much more counterproductive for a civilian population who may panic if not accustomed to an alarm and is likely to protest and become noncompliant if subjected to repeated false alarms.

For decisionmakers, the economic and political damage from civilian false alarms can quickly become intolerable. This is known in the field, sardonically, as "detect to regret." If false positives trigger high-regret actions, they will create an aversion to act on information and a distrust of the technology and the responsible agencies. In this circumstance, the risks of dissension and loss of confidence in government in the wake of an attack are heightened because it may subsequently be shown that a detection alarm was sounded but disregarded because of a history of false alarm ("wolfing").

As a result, our detector programs, developed initially primarily for the military, have become more engaged with the false positive problem as they have been pressed into civilian use. The problem they confront is that strategies to reduce false positives increase system costs (because more tests, and more varieties of tests, cost more money), they increase the delay in warning about attack (because extra tests take extra time), and they increase the likelihood that we will screen out real attacks.

Unfortunately, the likelihood of false positives is much higher than a policymaker might at first expect or find tolerable. Bayes' Theorem, a technical mathematical proposition, calculates the probabilities. For the layman, the logic of this theorem can be made apparent by the following example.

Assume that a detector system has an error rate of 1 percent, samples the atmosphere once per hour, and is so widespread and sensitive that any attack would hit the system in the range in which it operated. There are 8,760 hours in a year. If a city protected by such a system were attacked once in a year for five hours, there would be five sample times during which the alarm would signal an attack. With a failure rate of 1 percent, the chances would be only 1 in 100 that the system failed to detect the attack in its first hour.[48]

Even in the absence of a systemic problem, there is a major difficulty, however, when one considers the other 8,755 hours of the year (that is, the hours during which the city was not being attacked).[49] During 8,667 hours (99 percent of this time), the alarm would, quite correctly, not sound. During 88 hours (based on the 1 percent false positive rate), however, the alarm would sound incorrectly. If each alarm triggered a high regret action, the false alarm problem would be profound.

The period of non-attack is so much larger than the period of attack that the small percentage of false positives dominates the larger percentage of true positives: when the alarm rings it will be 17 times more likely to be a false alarm than a true one.[50] Under these assumptions, a program that equipped 10 cities with detectors when only 1 was attacked during a year would have, on average, 175 false alarms while alerting to 1 real attack.[51] To bring the system to the point where 5 in 6 alarms were true (that is, the false positive rate were only 1 in 6), the false positive rate would have to be 1 in 100,000.

The suppositions underlying this particular example can be debated; however, the general point that it illustrates should be clear. The false positive problem is substantial. To deal with it, and to keep costs within bounds, our most sophisticated detection systems layer technologies on top of one another. They first identify the presence of respirable particles in an air sample and then utilize laser florescence to determine whether these are biological particles.[52] Depending on the sensitivity at which it is set and on environmental circumstances, this technology has been found to trigger a concern between 1 and 10 times a day. In our most sophisticated systems, this "positive" initiates an automated process for a different kind of test. The sample is liquefied and tested against antibodies known to respond to identified biological agents. If the automated result signals an attack, a radio signal summons an operator who manually repeats the test. The operating office that directs one of these systems for which experience has been accumulated reports that after this is done, false positives still arise on the order of 1 in every 10,000 tests.[53]

Since this rate is unacceptably high for broad scale civilian response, positive samples are now taken to back up laboratories that perform polymerase chain reaction (PCR) tests to assess the DNA within the sample. In a representative operating system each test costs on the order of $30 and typically requires about 6 hours for a sample to be brought to the laboratory, prepared for PCR, and tested.[54] Though much more reliable than the field assays, a PCR test may generate false positives (though perhaps at a rate on the order of 1 in 50,000) because of contamination or difficulty distinguishing certain agents. The medical community does not yet accept the outcome of these tests as a conclusive judgment about the presence of a biological agent.[55] Moreover, a PCR test cannot determine whether an agent is alive. As a result, a positive PCR then leads, for bacterial agents, to a so-called gold standard test—that is, the growth of the agent in a microbiological culture media culture. That process typically costs about the same as a PCR test and takes 24 to 36 hours.[56] Only then is our information sufficient to permit a confident judgment that we have been subject to attack.[57]

This description should make it evident that the design and operation of systems to detect biological attack requires striking a balance between warning time, cost, sensitivity, and rate of false alarms. Determining this balance requires policy judgments. I will offer some recommendations in this regard after the discussion of windows of reward below. But, for the present, it is sufficient to note that a false alarm may be tolerable if it leads to nothing but a police force alert but intolerable if it triggers mass panic. Understanding (and creative design) of our response systems should therefore be inseparably linked to the design of our detector systems. The whole case must be understood in order to make a judgment about this part of it.

Moreover, we need to make more than one judgment about acceptable warning times, sensitivities, and false positive rates. Not only will these vary between cases, but also an informed decision-maker would be well advised to design the system to operate one way in advance of any attack but—recognizing reload—in quite a different way after an initial attack.[58]

Because of the risk of reload, paradoxically, detectors will be more valued—and valuable—after an attack than before it. Though efforts to warn a civilian population are now regarded as too imperfect and too costly to be implemented, it appears likely that after a first attack (and especially after repeated attacks), authorities will try to detect to warn whatever the

Recommendations

1. Establish planning scenarios and set resource requirements on the assumption that biological weapons will permit terrorists to rapidly "reload" and repeatedly attack. In this light, we must prepare for biological attacks repeated in different American cities rather rapidly after one another. Plan to defend against a campaign, not just an attack.

2. Use four attack cases (aerosol anthrax, aerosol smallpox, botulinum in drinks, and foot and mouth disease) as the planning premises for near-term work on bioterrorism throughout the Federal Government. Build a portfolio of required capabilities from these cases; test hypotheses about improvements to our defenses by assessing their value in dealing with these cases; measure progress against these cases.

3. The cases will be too limiting over the longer term as biological knowledge evolves and disperses, terrorists respond to our strengths and weaknesses, etc. To counter this, fund broad-ranging (as well as case specific) research and development and, wherever possible, favor multivalent defenses over narrowly targeted activities. In addition, establish a "Case 5 Committee" of scientists and intelligence officers. Charge the committee with regularly reviewing the evolution of biology and of terrorist group and state activities relevant to bioterrorism. Have the committee identify indicators and warnings of the evolution of new threats, recommend intelligence efforts to document the evolution of those threats, and change the cases as warranted over the years ahead.

4. Though local first responders are important, recognize that the Federal role is central in responding to major bioterrorist attacks. Immediately establish a Federal biological emergency support team whose members (our leading experts from government and the private sector) have the range of skills and knowledge to support senior decisionmakers in the event of a biological attack. Train the team using the planning cases and have it deepen insight into resources and strategies that will be helpful to cope with these cases. Support the team and senior decisionmakers with the required information and communication systems.

5. Recognize that an anthrax attack can readily be mounted with an antibiotic resistant strain. Establish a goal of developing a triad of antibiotic, vaccine, and a third response (for example, lysins, bacteriophages, or antitoxins) to anthrax. Diversify the antibiotic stockpile as much as possible. Accelerate the development of a new anthrax vaccine. In the interim, expand stockpiles of the existing anthrax

state of our detector capabilities.[59] They will also detect to reassure—detectors will be valued to tell residents of other cities that they have *not* been attacked. To achieve this, it appears likely that after a first attack we will increase our sampling (thus raising the number of false positives reported by individual detectors), we will raise the costs of false positives (because they will more probably rapidly lead to reactions), and we will more readily tolerate these costs.[60] Accordingly, we should develop alternative plans for detector operation, including alternative standards for trade-offs between false positives, sensitivity and speed. One approach will apply to the present situation and another will apply if an attack has occurred and we are confronting reload.

Senior officials need now to grasp these problems, to make the requisite judgments, and to provide guidance to those working on the technical aspects of detection problems.

Necessarily, these judgments must be made at the Federal level,[61] probably in the new Department of Homeland Security. To the extent that detector programs remain within the purview of the Department of Defense, interagency coordination and cooperation are required. Until that is achieved, the deployment of a useful detector capability will be difficult.

Recommendation 6: Establish cost, false positive, and sampling expectations for detector and laboratory systems with the goal of detecting to treat in the present environment. Recognize that, after an aerosol attack, concern about reload will create a demand for more intensive sampling and less stringent false positive and cost standards. In that environment, detect to warn may become our goal. Target detector and laboratory investments and design detector and laboratory systems so that they respond to present priorities but can also quickly be adapted to post-attack priorities.

Detection Speed: The Window of Reward

The cases bring home the importance of time. Of course, earlier detection of a biological attack is always more valuable than later detection. However, the increments in reward from greater speed are not smooth across all time frames. As a result, windows of reward (that is, time phases in which we gain particular benefit from detection) can be identified for detectors in each of these scenarios. The requirements to be established for our detector programs under the previous recommendation should focus on producing useable results within windows of reward.

As noted, detect to warn within the first minutes or few hours of attack is very difficult to achieve. But there is a form of detect to warn against an aerosol anthrax attack that may be achievable in a period of

vaccine. Begin production of a chosen third-response drug as soon as possible.

6. Establish two sets of cost, false positive, and sampling operating requirements for detector systems, one for the present environment and the other for a post-attack environment. Recognize that after an aerosol attack, perception about the ease of reload will create a demand for more intensive sampling and less stringent false positive and cost standards. Target detector and laboratory investments and design these systems so that they not only respond to present priorities but can also quickly be adapted to meet anticipated increased post-attack demands.

7. Establish a requirement and allocate funding to improve our detection systems (including confirmatory polymerase chain reaction or other nucleic acid tests) to achieve a reliable anthrax alert within 8 to 10 hours. Tie this to an alert system that would warn the population to stay indoors. When these systems have been adequately demonstrated, engage industry in a competition to build and operate the specified detection systems.

8. Prepare for, and in the event of an attack expect simultaneously to initiate, both a national mass vaccination campaign and a local campaign to identify those who may be exposed to smallpox. Give great priority to developing a second-generation smallpox vaccine that will enable broader, less risky vaccination.

9. If a smallpox threat is judged to be significant, then establish an integrated Federal system capable, within 96 hours of a smallpox attack on a major urban area, of both detecting that attack and vaccinating the population likely to have been infected.

10. Commission research and development projects to produce a diagnostic test capable of identifying smallpox in infected individuals within the first 4 days of exposure.

11. If a smallpox threat is judged to be significant, then offer the option of a smallpox inoculation to Americans whose health profiles indicate that they are not substantially at risk from the vaccine.

12. Use a DISC System to systematically evaluate progress in developing the capabilities that are critical to our defense against bioterrorism. Develop a DISC Report for each case. Use the DISC system as a framework for highlighting and then debating our spending priorities.

6 to 10 hours after an anthrax attack. This is because an urban aerosol anthrax attack is most likely to occur at dusk, when weather patterns are most favorable to keeping the anthrax close to the ground and therefore likely to be inhaled as it disperses.[62] An overnight ability to ascertain that an attack has occurred could trigger a warning to stay at home, reducing doses received and avoiding the contamination of inbound commuters, school children, and others who were not exposed in the first attack. Such a warning could also minimize activities (like street sweeping) that would be most likely to provoke reaerosolization. A warning of this kind would be relatively easy to communicate: the mechanisms would be like those for a snow day.

Unfortunately, present anthrax detector capabilities do not now deliver actionable results within this window of reward.[63] The problems are partly issues of collection frequency, partly of speed, and partly of reliability. Because of cost considerations, many detector systems are not automated and are manually sampled only every 12 or 24 hours.[64] On average, accordingly, the material from these systems is 6 or 12 hours old and subject to some significant travel time even before it begins to be assessed. This can be dealt with, at a significant financial cost by increasing the sampling rate, by automating detection, or (probably most attractively) by mixing strategies such as using automated systems and other threat indicators as triggers to accelerate the frequency of manual collection. But, as described in the previous section, even automated systems now require a manual check, then transport to a laboratory, preparation for a PCR test, PCR testing, and culturing. These can be accelerated, but now typically take between 1 and 2 days.

Ironically, this not only leaves present anthrax detector systems outside the desired window of reward for protection of large civilian populations but also renders them of marginal utility as instruments for giving actionable warning for a mass response to an attack. As noted above, it is probable that within 48 hours after an aerosol anthrax attack[65], the first 5 percent of those infected will manifest substantial flu-like symptoms.[66] There are five major emergency rooms in the Washington, DC, area. On average, each sees 200 patients a day. If 5 percent of 200,000 infected individuals develop flu-like symptoms within 48 hours, approximately 10,000 people will be ill by the end of this period. If a quarter of those come to the major emergency rooms, patient numbers will more than triple. If 10 percent come to these emergency rooms, those numbers will double. In the present security environment, these circumstances would very probably prompt consideration of whether we had been attacked. For patients who develop the disease rapidly, a blood culture will, within as soon as 3 or 4 hours, provide a clear indication that an anthrax attack has occurred.[67] Accordingly, under normal operating conditions our detector systems are likely to produce conclusive results only a little ahead of (though with more certainty than) our emergency rooms.

Managers of the detector research and development programs and higher level policymakers would be well served by recognizing that the present anthrax aerosol detection capability, though valuable for building alerts and for forensic and epidemiological purposes, must be accelerated if it is to contribute significantly to a city-wide alert. The most attractive path to this result would appear to be through automation of detectors and/or PCR preparation, as well as determination of whether the error rate of the PCR test can be reduced to acceptable levels.[68] It would enhance the prospect of value from these systems if requirements were focused on the 8-to-10-hour window of reward, providing overnight notice. Establishing such an explicit requirement, along with the previously recommended standards for false positive rates and other variables, would pave the way to deciding how much we were willing to pay for such systems and how broadly and rapidly we wanted to deploy them. Only when those decisions are made will we be able to secure the broad scale industry participation in this endeavor that can sustain large systems and bring costs down.

Recommendation 7: Establish a requirement and allocate funding to improve detection systems (including confirmatory PCR or other nucleic acid tests) to achieve a reliable anthrax alert within 8 to 10 hours under normal operating conditions. Tie this to an alert system that would warn the population to stay indoors. When these systems have been adequately demonstrated, engage industry in a competition to build and operate the specified detection systems.

The Smallpox Case[69]

Assumptions

This case assumes an aerosol attack such as the *B. anthracis* bacteria attack described in case 1, but disseminating the smallpox virus instead of anthrax. It assumes, as in case 1, that 200,000 individuals are

infected in the primary exposure area, but in this instance the first 5 percent of individuals do not manifest symptoms until 7 days, and the average case does not manifest signs or symptoms until the 12th day. There is no treatment that is more than palliative after symptoms appear, and individuals become infectious when they manifest symptoms. The mortality rate is 30 percent. Newly infected individuals will themselves become infectious after 10 to 12 days and may remain ambulatory for as much as 48 hours during this infectious period. If not isolated, each such individual will infect several second-generation cases.

Observations and Recommendations

National Mass Vaccination vs. Local Targeted Vaccination and the Need for a New Vaccine

An intense debate is being conducted over whether the well-practiced technique of local ring vaccination would be sufficient in the wake of a smallpox attack or whether national mass vaccination would be required.[70] A parallel debate exists over whether broad scale vaccination should be undertaken in advance of an attack, with proponents emphasizing the risk of attack and opponents arguing that post-attack vaccination can be accomplished with sufficient rapidity, while pre-attack vaccination will engender vaccine related illnesses and deaths. We will return to the second debate later. Let us focus, for the moment, on the first issue.

In the event of an aerosol attack, neither a national mass vaccination campaign nor a targeted local campaign substitutes for the other. To the contrary, both are required. If mass national vaccination had not already occurred, it would be required in the wake of an attack because it would quickly be realized (and perhaps demonstrated) that the attacker could attack again and again in different places. Since smallpox no longer occurs naturally, just one case would indicate that an attack has occurred. When the ability to reload is recognized, populations outside the area of attack will be regarded (and will regard themselves) as vulnerable. That sense of vulnerability will be enhanced by a substantial number of ambiguous cases (measles or chicken-pox, for example). As described at greater length below, no test exists that allows us to determine whether someone is infected with smallpox before he or she begins to manifest symptoms some 7 to 12 days after infection. Against a backdrop of reload capability, this uncertainty very likely would trigger national mass vaccination, even if local vaccination would alone control the recognized cases.

However, with the present live-virus vaccine, even if mass vaccination had already occurred, on the order of 20 to 60 million Americans (for example, immune deficient individuals, those who suffer from skin diseases, pregnant women, small children, people who are receiving certain cancer treatments, and those who live with such individuals) would not be vaccinated absent direct exposure to smallpox. This underscores the need to develop a second-generation pure protein or other improved vaccine that could be administered to these populations. For the moment, however, mass vaccination will still leave as much as 20 percent of our population vulnerable. Moreover, there will be large numbers of transient non-citizens, individuals who refuse[71] or evade[72] vaccination, and individuals whose vaccination did not take or whose immunity deteriorated. In the wake of an attack (which may be a second or third or fourth attack after the initial outbreak), a local review will be required to determine who was likely to have been exposed. Identification and vaccination of those who were previously missed will be a priority effort. Therefore, it is imperative to assume that in the event of an attack, we will conduct both comprehensive (mass national) and specific (local) vaccination campaigns.

Recommendation 8: Prepare for, and in the event of an attack, expect simultaneously to initiate, both a national mass vaccination campaign and a local campaign to identify those who may be exposed to smallpox. Give great priority to developing a second-generation vaccine that will enable broader, less risky, vaccination.

Window of Reward for Detection

For smallpox, 24 to 48 hours is the window of reward for detection. While the window of reward for anthrax was based on an opportunity to detect to protect, the smallpox window of reward is based on detect to treat. This is because a smallpox vaccination administered within approximately 96 hours after an attack is likely to protect an exposed person, while immunization after that point is much less likely to be effective[73]—and we have no subsequent method of effective treatment.[74] Accordingly, a 24- to 48-hour alert system with an acceptably low false positive rate will yield immense benefits if it is linked to a consequence management system that is geared to inoculate exposed persons within the subsequent 48 to 72 hours.

The technology for such a detector system is now in hand. As with anthrax, if detectors were in place, the timeline for confirmed detection of an aerosol smallpox attack would likely be on the order of 24 to 36 hours. In contrast to anthrax, detection within this period would yield warning well in advance of the appearance of the first patients.

Unfortunately, our detector systems are not linked to a civilian alert and treatment system that would take advantage of a smallpox window of reward warning. To the contrary, under the present system, notifications would be made to a number of city, county, state, and Federal authorities, none of which has the ability to direct and achieve widespread smallpox vaccination during the critical 48 to 72 hours. Federal vaccination plans (an admirable contribution to our biodefense capabilities) are focused on ring and mass vaccination on the premise that smallpox cases have broken out and that vaccination is a means of protection against infection not yet incurred. They are therefore notably less urgent and less broad scale than the case suggests would be required. The Centers for Disease Control and Prevention has made a good start in requesting plans from each major metropolitan area to establish, on demand, 20 clinics capable of vaccinating 118,000 people per day. Over the longer term, it has the ambitious goal of being able to vaccinate a million people in an area within 5 days and the entire U.S. population within 15 days. But if an aerosol attack occurred, for example, in Washington, DC, only a small fraction of the metropolitan area's 3.5 million citizens could be vaccinated within the required 96-hour window.

No sufficiently speedy mechanism now exists for a decision to vaccinate after aerosol detection; our information about an attack is likely to be too limited to map the likely shape and course of an infectious cloud so as to discriminate confidently as to whom to vaccinate[75]; and our vaccination systems are not robust enough to achieve mass vaccination within four days of an attack.

The present course of action in the wake of 24-to-48-hour detection of an aerosol attack would probably be counterproductive in three critical respects. First, panic would ensue as word of the attack spread and it became evident that the Government had only an inadequately slow plan for dealing with it. Second, there would be a divisive disparity between those whom Government protected and those whom it did not. Privileged individuals—particularly those who benefited from official positions—would be vaccinated. This would include Members of Congress, military leaders, and civilians in senior positions in national, and perhaps state and city, government. Many, if not all, ordinary citizens who were exposed would not get inoculations in time. Third, even if vaccinations were randomly distributed, there would be an extraordinary protest over government failure to plan an effective distribution.

Viewed through the lens suggested in the introduction, all these outcomes would amplify the effects of a terrorist attack, decreasing confidence in the government and increasing the distraction from divisiveness and panic.

Recommendation 9: If a smallpox threat is judged to be significant, then establish a requirement for an integrated Federal system capable, within 96 hours of a smallpox attack on a major urban area, of both detecting that attack and vaccinating the population likely to have been infected.[76] If adequately resourced and carefully prepared, such a system should be feasible with existing technologies.

First 96-Hour Diagnostic Test

Our response to a smallpox attack can be greatly improved by developing a test to reveal smallpox within the first 96 hours after an individual has been infected. No such diagnostic now exists[77], nor has the time priority been clearly established, but such a diagnostic is scientifically plausible. If available, it would permit us to confine vaccination of immune deficient and other contra-indicated individuals only to cases of actual infection, thereby avoiding a draconian choice as to whether to vaccinate—a choice which can now be made only in ignorance. Furthermore, such a test could enable us to focus our resources for isolation, vaccination, and treatment to the extent that these became necessary. Perhaps most significantly, such a test would indicate whether an individual or a population had been attacked. In the absence of adequate detector information, it could be an important means of reassurance or a trigger for immediate immunization.[78]

Recommendation 10: Commission research and development projects to produce a diagnostic test capable of identifying smallpox in infected individuals within the first 4 days of exposure.

Voluntary Vaccination Options in Advance of an Attack

In determining whether the option of smallpox vaccination should be provided to Americans in advance of an attack, three issues have been discussed, but a fourth has been largely ignored. The

three properly discussed issues are the likelihood of the threat, the number of illnesses and fatalities likely to be caused by vaccination, and the speed with which we could vaccinate those who have not been infected. But the silent fourth issue is the character and availability of present detector and response systems and, therefore, our ability, in the event of an attack, to protect those who have already been infected. If detector and response systems are firmly enough established and widely enough disseminated to vaccinate within 96 hours of an attack, there may be no compelling reason to give ordinary citizens the opportunity for prior vaccination. Conversely, if we do not finance and secure such systems, the case for providing this opportunity is much stronger.

The technology is available for the detector portion of this system. Post-infection vaccination within 96 hours can possibly be achieved. But, as noted, the vaccination capabilities are not now in place. Moreover, to be relied upon, such a system would have to be broadly installed and frequently sampled, at substantial cost. In the foreseeable future, it would very likely have gaps in suburban and rural areas.

The resolution of the debate involves a policy judgment. But appreciation of the aerosol threat, of reload capabilities, and of the difficulties in detector and response coverage tilts the argument toward permitting voluntary vaccination if the threat is regarded as significant. Put another way, the case against offering the option of pre-attack vaccination depends on the judgment that post-attack mass vaccination can be achieved in the necessary time window. If an attack is manifested by a few hundred cases (most probably caused by an infectious individual) then the period for protecting society from second-generation cases will be approximately 96 hours for the limited number who were already infected and longer for those who were not yet infected. Opponents of prior mass vaccination have implicitly assumed this case. But if an aerosol attack occurs, then detection must occur, with reasonable assurance and near omnipresence, within 24 to 48 hours, and several million people must be vaccinated within the next 48 to 72 hours. Those two criteria are difficult to meet. Sensitivity to the aerosol case pushes us toward permitting pre-attack vaccination.[79] Moreover, the chances of meeting these criteria are greater if some substantial prior vaccination has occurred.

Recommendation 11: If a smallpox threat is judged to be significant, then offer the option of a smallpox inoculation to Americans whose health profiles indicate that they are not substantially at risk from the vaccine.

Section 5

Capabilities

Our abilities to detect a biological agent and to counter it through drugs and vaccines are two amongst a number of required capabilities. As a simple mechanism for highlighting and recording these capabilities, I suggest that Federal and local governments employ a "DISC Decathlon." DISC is an acronym composing what I regard as the 10 (that is why it is labeled "a Decathlon") most critical capabilities. These are:

- Detection
- Drugs and vaccines[80]
- Decontamination[81]
- Interdiction[82]
- Intelligence[83]
- Surveillance and diagnosis[84]
- Simulation, modeling, and gaming[85]
- Counterproliferation[86]
- Civilian preparation[87]
- Consequence management[88]

This paper has discussed the first two categories (detection and drugs and vaccines) in some detail, touching as well on some important consequence management issues. Additional work, however, is warranted in all areas. If these areas are defined and agreed upon, they can be the focus of work within Federal agencies, at national laboratories, in selected think tanks and universities, and among contractors. Used in conjunction with the designated cases, these topics can provide the basis for training and planning.

Figure 1. DISC Report for Anthrax

Contributor	Now	Mid	Long	Comment
Detection	2/$?	3/$?	5/$?	Focus on window of reward
Drugs and vaccines	5/$?	7/$?	4/$?	Improve vacc. & AB distrib. methods; genetic eng threat
Decontamination	1/$?	2/$?	4/$?	Must build large scale capability
Interdiction	0/$?	0/$?	1/$?	Imperative to rethink
Intelligence	2/$?	3/$?	4/$?	Case 5 Committee; classified technology improvements
Surveillance and diagnosis	7/$?	8/$?	9/$?	Can significant improvements be made?
Simulation, modeling, gaming	2/$?	7/$?	9/$?	Weather and human models
Counterproliferation	1/$?	1/$?	2/$?	Difficult to impossible?
Civilian Preparation	0/$?	2/$?	4/$?	Filters? Education?
Consequence management	1/$?	2/$?	4/$?	Rich requirements and opportunities; invest in Fed prep

It should also be possible for the Department of Homeland Security, or another Federal agency designated by the President, to develop a DISC report for each case of concern. Such an assessment could briefly summarize the present contribution of each capability to defense under each of the cases. An element that made no contribution might receive a ranking of zero, while one that could be expected to make a great contribution might receive a 10, with others falling in between. A DISC report could also project, under present trends, how these elements would be likely to contribute in the midterm (2–5 years) and longer term (6–10 years). Finally, each report could give us a very approximate, but very valuable, picture of how we are investing to counter the threat, by estimating the dollars we are (or will be) spending to develop the relevant capabilities. The result will be a functional portrait of our capabilities and our prospects. This will prove a basis for debating whether we are making the right investments at the right levels.

DISC reports might look like the example for anthrax on the previous page (figure 1) and the example for smallpox below (figure 2).

These numbers should not be taken too seriously. They are merely illustrative of how a DISC report may comprehensively, but simply, illuminate a case. The reports highlight, for example, that our drugs and vaccines are now useful against anthrax and smallpox, but that on present trends, while our smallpox arsenal can be expected to become more useful (with a better vaccine and the development of antivirals), our anthrax arsenal is likely to grow less so (as attackers are more likely to employ genetic engineering skills.)[89] The reports underscore the need for focus on windows of reward in our detector programs; they make salient the need for clarity in plans respecting decontamination, etc. These estimates are the beginning of a discussion, not its end. Put another way, they provide a framework for considering where we are and where we are going.

Recommendation 12: Use the DISC system to evaluate systematically the capabilities that are critical to our defense against bioterrorism. Develop a DISC report for each case. These reports will permit us to see where we are spending money and to make some judgments about where we should be spending more or less.

Figure 2. DISC Report for Smallpox

Contributor	Now	Mid	Long	Comment
Detection	3/$?	5/$?	6/$?	Focus on window of reward
Drugs and vaccines	5/$?	7/$?	9/$?	New vacc and anti-virals; mr robust pre-attack vacc. and/or standby cap
Decontamination	3/$?	5/$?	6/$?	Naturally degrades; but enclosed spaces (e.g., subway)?
Interdiction	0/$?	0/$?	1/$?	Imperative to rethink
Intelligence	2/$?	3/$?	4/$?	Case 5 Comm.; classified technological improvements
Surveillance and diagnosis	3/$?	3/$?	8/$?	Early diagnosis technology
Simulation, modeling, gaming	2/$?	7/$?	9/$?	Weather and human models
Counter proliferation	9/$?	9/$?	9/$?	Near optimal; moral consensus; limited availability
Civilian preparation	0/$?	2/$?	4/$?	Preemptive vaccination?
Consequence management	2/$?	3/$?	3/$?	Rich requirements and opportunities; invest in Federal preparation.

Section 6

Conclusion

This paper demonstrates that the case/capabilities approach provides a valuable framework for our efforts to defend against bioterrorism. The precise character of the cases used is, of course, subject to debate and may be further refined now[90] and then change over time. However, for the near term, the four specified cases (aerosol anthrax, aerosol smallpox, botulinum, and foot and mouth disease) address the most salient and significant problems and provide a broad enough range to orchestrate U.S. Government planning appropriately. I believe that a broad consensus can be achieved in support of making these (or other cases very like these) our priority planning premises.

The methods utilized in this paper to analyze drugs and detectors can be employed to assess other capabilities critical to our defenses against bioterrorism. In the immediately preceding section, I have outlined the capabilities that I believe should receive priority. If we pursue this mode of thought, I believe that we can (a) create a unified understanding of the field; (b) test hypotheses in light of that understanding; (c) establish broadly accepted priorities and goals; (d) measure progress against these goals. The result will be a better ability to defend ourselves against an appalling threat.

Endnotes

[1] As a general matter, people speak of biological warfare when living organisms (usually microscopic) or their products or components are used as weapons. This categorization is somewhat awkward. Ricin, for example, is commonly referred to as a biological weapon because it is a toxin (that is, a poison) that is produced from castor seeds. To accommodate this and other toxins, the relevant international convention is called the Biological and Toxin Weapons Convention. But Ricin can be manufactured synthetically and is accordingly also regulated under the Chemical Arms Control Convention. Moreover, future biological weapons may utilize pathogens that are not bacteria, viruses, or toxins (for example, prions or bioregulators). For the moment, however, this definition will suffice.

[2] An excellent overview of America's responses to the threat of chemical and biological terrorism employed a similar metaphor. See Amy E. Smithson and Leslie-Anne Levy, *Ataxia: The Chemical and Biological Terrorism Threat and the US Response*, Stimson Center Report 35 (Washington, DC: The Henry L. Stimson Center, October 2000). On its title page the report offers the following definition of *ataxia*: "n 1: lack of order: CONFUSION; 2: an inability to coordinate voluntary muscular movements that is symptomatic of some nervous disorders."

[3] Others are trying to improve coordination by organizational changes, including, most notably, by establishing the new Department of Homeland Security. But the premise of this section is that such efforts cannot displace the need for a common conceptual framework. Within its own branches and divisions, the new department itself requires common planning premises and, externally, it must work alongside established entities (such as the Department of Health and Human Services, the Department of Defense, and so forth). These efforts can only be effective if they are unified.

[4] An invaluable summary of the history is provided by W. Seth Carus, *Bioterrorism and BioCrimes: The Illicit Use of Biological Agents Since 1900* (Washington, DC: Center for Counterproliferation Research, National Defense University, February 2001). See also Erhard Geisster and John Ellis van Courtland Moon, *Biological and Toxin Weapons: Research, Development and Use from the Middle Ages to 1945,* Stockholm International Peace Research Institute, Chemical and Biological Warfare Studies No. 18 (Stockholm: Oxford University Press, 1999).

[5] Though increases in volume may require modifications in production "recipes" and increase the risk that an effort will be noticed.

[6] Some have argued that the threat of nuclear retaliation can be sufficient to deter bioterrorism. Unfortunately, this proposition cannot be sustained. We ordinarily have a high standard of attribution before retaliation. Only after years of painstaking work did we feel so confident in attributing the Lockerbie Pan Am bombing to Libya that we retaliated. Terrorist groups and their state sponsors are the most difficult actors to identify, and biological weapons delivered by covert means (rather than missiles) are the most difficult weapons to attribute. The first phenomenon is well illustrated by the debate about Iraq's connection to September 11, the latter by the still unresolved attribution debate about the anthrax letters. Moreover, terrorists, or even a head of state if he were in extremis, might seek to provoke nuclear attack so as to upset other U.S. military plans (such as an ongoing invasion of his country) or stimulate outrage against the United States.

[7] Like so many other "facts" taken as benchmarks in the realm of bioterrorism, this is subject to debate. The generalization derives from studies of healthy "middle-aged" primates. The *Journal of the American Medical Association* consensus statement on anthrax concludes: "Extrapolations from animal data suggest that the human LD_{50} (i.e., dose sufficient to kill 50 percent of persons exposed to it) is 2,500 to 55,000 inhaled *B anthracis* spores. The LD_{10} was as low as 100 spores in a series of monkeys." See Thomas V. Inglesby et al., "Anthrax as a Biological Weapon, 2002: Updated Recommendations for Management," *Journal of the American Medical Association* 287, no. 17 (May 1, 2002), 2236–2252.

[8] "[U]ncertainties of a factor of 10 or more in the LD_{50} values and a factor of 2 or more in the probit slopes (i.e., the dose response curves) for different agents are common. These uncertainties are even greater if the strain type is not known or the mechanism and magnitude of environmental decay rates for different agents is not understood. Moreover, the incubation period (and its dose dependence) for different agents can vary by factors of 2 or more; and diurnal and weather variations can easily affect the contaminated area by an order of magnitude or more for open air releases. . . . Finally, uncertainties surrounding the amount and purity of the agent, the aerosolization efficiency . . . reaerosolization . . . protection factors . . . and breathing rates can easily affect the inhaled dose by an order of magnitude or more." National Research Council, *Making the Nation Safer* (Washington, DC: National Academy Press, 2002), 81.

[9] Though weather conditions would affect abilities to attack particular targets at particular times.

[10] The very limited anthrax mailings in September and October of 2001 stretched the Centers for Disease Control and Prevention and other national public health resources near the limit. Fire, hazardous material response teams, laboratory, and law enforcement resources were severely strained responding to

citizen reports of white powders. Our decontamination capacity, likely to be in heavy demand in the wake of an aerosol anthrax attack, is so taxed by the task of decontaminating the Brentwood Postal Facility in Washington, DC, that no start has been made on decontaminating a New Jersey postal facility. From these and other examples, it is evident that our national resources are not sized to cope with reload.

[11] I am indebted to Larry Gershwin of the Central Intelligence Agency for suggesting this campaign terminology. I am also grateful to Brad Roberts at the Institute for Defense Analysis for sharing his thinking as IDA institutes a study of "campaign terrorism."

[12] History suggests that when nations do not have an offensive plan for a particular weapon, they undervalue the likelihood that others will use it and even dismiss instances of use as accidents or irrelevant events. See generally, Jeffrey W. Legro, "Military Culture and Inadvertent Escalation in World War II," *International Security* 18 (Spring 1994), 108–142.

[13] See Friedrich Nietzsche, "The Wanderer and His Shadow,"in *The Portable Nietzsche,* ed. Walter Kaufman (New York: Viking Press, 1977). Nietzsche wrote, "Along the journey we commonly forget its goal. Almost every vocation is chosen and entered upon as a means to a purpose but is ultimately continued as a final purpose in itself. Forgetting our objectives is the most frequent stupidity in which we indulge ourselves."

[14] I am indebted to Ralph Gomory for this observation.

[15] Furthermore, as described below, the cases will change over time because warfare is dynamic—as we grow stronger in some respects, terrorists will open new avenues of attack. Methods of attack will also change as biological understanding and the techniques of genetic manipulation continue to accelerate and are ever more widely dispersed. We cannot assume that attack will occur in the manner anticipated by a case.

[16] The planning cases should, accordingly, be neither be so easy as to oversimplify the problem, nor so hopeless as to make action irrelevant.

[17] The Defense Science Board Task Force on Bioterrorism embraced my recommendation in this respect. See *Report of the Defense Science Board Task Force on Homeland Defense against Bioterrorism*, November 2002, 4–5.

[18] Shortly before this paper went to press, D.A. Henderson suggested that it might be more fruitful to vary the cases further by using a building air filter attack and/or a subway attack as the second (smallpox) case. This suggestion has merit and should be explored in future studies.

[19] We also need to remain sensitive to the risks of cases that might be outside this range, for example, Ebola, SEB, or more futuristic threats. Methods for accomplishing this, both in our research and development programs and in the evolution of our planning premises are discussed below.

[20] As noted above, a first order issue will be to take account of reload in establishing these requirements.

[21] Genetic sequencing and supercomputing should ultimately make all pathogens subject to modeling and analysis. It is likely, however, to be a long route to achieve this goal.

[22] *Prions* are proteins and protein fragments that physically disrupt the folding of proteins naturally present on the surface of some cells in mammals. They appear to be the causative factor in "mad cow disease," Creuzfeld-Jakob Disease, and perhaps Alzheimer's Disease. Prions are extremely resistant to decontamination techniques, including standard autoclaving and the use of bleach or other oxidants.

[23] In healthy humans, *bioregulators* stimulate and retard physiological processes such as inflammation, clotting, or nervous system response. An excess of a bioregulators, introduced by aerosol or other means, could (like toxins) produce fatal or disabling consequences. Peptide bioregulators may (through fatigue and mood) affect the will or ability to act.

[24] See generally, Steven M. Block, "Living Nightmares: Biological Threats Enabled by Molecular Biology" in *The New Terror*, ed. Sidney Drell et al. (Stanford: Hoover Institution Press, 1999), 39–75.

[25] Future work will turn to the botulinum and foot and mouth cases. Readers interested in the botulinum case may see Stephen S. Arnon, "Botulinum Toxin as a Bioweapon," in *Biological Threats and Terrorism: Assessing the Science and Response Capabilities,* ed. Stacey Knobler et al. (Washington, DC: National Academy Press, 2002), 57–63; Arnon et al., "Botulinum Toxin as a Biological Weapon: Medical and Public Health Management, Consensus Statement," *Journal of the American Medical Association* 285, no. 8 (February 28, 2001), 1059, 1070; and, more generally, "Terrorist threats to food: guidance for establishing and strengthening prevention and response systems," (World Health Organization, 2002), ISBN 92 4 154584 4, NLM classification: WA 701; "Food Safety and Security," GAO Report to Congress, October 10, 2001. Readers interested in the foot and mouth disease case may examine Michael E. Peterson, "Agroterrorism and Foot and Mouth Disease: Is the United States Prepared?" in *The Gathering Biological Storm,* ed. Jim A. Davis and Barry R. Schneider (USAF Counterproliferation Center, 2002), 9–40; and, more generally, National Research Council, *Countering Agricultural Bioterrorism* (Washington, DC: National Academy Press, 2003); and Henry S. Parker, *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat,* McNair Paper No. 65 (Washington, DC: National Defense University Press, 2002).

[26] See generally Inglesby et al.

[27] The Defense against Weapons of Mass Destruction Act of 1996, 50 USC Section 2301ff, is commonly known as the Nunn-Lugar-Domenici Program. Smithson and Levy provide a useful (and skeptical) overview of the effort.

[28] The Public Health Security and Bioterrorism Preparedness and Response Act of 2002, for example, appropriated $1.1 billion to 62 states and territories and directly to New York, Chicago, and Los Angeles.

[29] This effort would also complement, but not displace, existing National Guard Civilian Support Teams. These 32 teams (a proposal now before Congress would expand the number to 55) are intended to advise on-the-scene incident commanders about spread, decontamination, containment, and related issues in the wake of the use of a weapon of mass destruction. It is remarkable that we have such teams for governors (at a cost of approximately $3.2 million per team per year) but have no expert support system for the Federal Government. The envisioned Federal biological emergency advisory team would operate at a higher level than the National Guard System, providing it with some consistent Federal guidance.

[30] The risk of illness can be diminished by inoculating members (and perhaps for psychological reasons members of their

immediate families) in advance against known agents. This is another reason for pre-selection of the team.

[31] I am indebted to Michael Osterholm for this formulation of the problem.

[32] See, for example, Ian Anderson, "Foot and Mouth Disease 2001: Lessons to Learned Inquiry Report" (London: House of Commons, 2002) commenting, in Section 9.4, on the workload in regional Disease Control Centers: "The outbreak was traumatic for everyone it touched. Many people sustained extreme working patterns, often 12 or more hours a day, seven days a week for long periods. . . . Some suffered breakdowns. Some are still suffering. . . . It was not until April that some managers began to understand the need for staff to take a break from their duties."

[33] Nor do we have good information about the effects of the anthrax vaccine on children, pregnant women, immune deficient individuals, and the elderly. The gaps in our vaccine supply (and understanding) are even greater for botulinum and foot and mouth disease. The toxins and viruses that cause these diseases come in different strains; our vaccines-in very limited supply-do not work against all strains.

[34] However, the development of antibiotic resistance may be accompanied by a lessening in agent virulence. It is likely to be difficult, particularly for a nonstate actor, to test virulence reliably. The pursuit of antibiotic resistance therefore introduces uncertainty for a terrorist as well as for us.

[35] Our limited antibiotic armamentarium relevant to anthrax is well documented and widely recognized. Our primary resources are ciprofloxacin (a fluoroquinolone), doxycycline (a tetracycline), and penicillin G.

[36] Itzhak Brook et al., "In vitro resistance of *Bacillus anthracis* Sterne to doxycycline, macrolides and quinolones," *International Journal of Antimicrobial Agents* 18, no. 6 (December 2001), 559–562. Antibiotic resistance can also be achieved by inserting an antibiotic resistant plasmid into *B. anthracis*. This is more challenging than the method described above, but is college-level biology and could more readily convey resistance to multiple antibiotics. In 1996, scientists from the State Research Institute of Applied Microbiology in Obelinsk, Russia, reported in open literature that they had developed a variant of the vaccine strain of anthrax "resistant to penicillin, rifampicine, tetracycline, chloramphenicol, macrolydes and lyncomicine by introducing recombinant plasmid pTEC, inheriting resistance genes to these antibiotics." See A.V. Stepanov et al., "Development of Novel Vaccines against Anthrax in Man," *Journal of Biotechnology* 44 (1996), 155, 157.

[37] Like much else in this field, this proposition is subject to dispute. Our data on immunization are limited and generally derived from tests on monkeys. See generally, Centers for Disease Control, "Use of Anthrax Vaccine in the United States," *Morbidity and Mortality Weekly Report* 49, no. RR–15 (December 15, 2000), especially 7 and sources cited there.

[38] Resistance to one antibiotic, ciprofloxacin for example, does not necessarily imply resistance to all antibiotics, but there are already naturally occurring strains that are resistant to the major alternative (and the historical treatment of choice), penicillin. Doxycycline may remain an alternative, but this is by no means assured, and the size of our stockpile will be diminished by the absence of the presently anticipated major alternative, ciprofloxacin.

[39] Two contractors have been engaged by the National Institute of Allergy and Infectious Diseases (NIAID) to produce a recombinant vaccine manufactured by modern methods. An improved vaccine is expected to halve the burden of the multi-inoculation series from six to three, but it is not likely to confer more rapid immunity. Working with university laboratories, DARPA is pursuing more far-reaching vaccine improvements that aim to exploit the recent genetic mapping of *B. anthracis*. The Navy Medical Research Center is working with the Battelle Institute to produce an anthrax DNA vaccine that they anticipate will be certified as an investigational new drug by the summer of 2003 and will require only two shots to establish immunity. Several researchers have suggested approaches that may be able to reduce dramatically the time from identification of pathogens to the production of a vaccine.

[40] See, for example, Raymond Schuch, Daniel Nelson, and Vincent A. Fischetti, "A bacteriolytic agent that detects and kills *Bacillus anthracis*," *Nature* 418, no. 6900 (August 22, 2002), 884–889; and B. Biswas et al., "Bacteriophage Therapy Rescues Mice Bacteremic from a Clinical Isolate of Vancomycin-Resistant *Enterococcus*," *Infection and Immunity* 70 (2002), 204–210.

[41] As a member of the Board of Directors of Human Genome Sciences, a NASDAQ listed company, I have encouraged the company in its efforts to develop an anthrax antitoxin. I do not believe that my views on this point are distorted by any financial interest, but readers will want to make their own determination. Under any conditions, alternative sources could supply antitoxin, and I make no representation as to which would be the best.

[42] A case for this approach is laid out in Arthur M. Friedlander, "Tackling Anthrax," *Nature* 414, no. 6860 (November 8, 2001), 160-161. See also M. Mourez, R.S. Kane, J. Mogridge, S. Metallo, P. Deschatelets, B.R. Sellman, G.M. Whitesides, R.J. Collier, "Designing a polyvalent inhibitor of anthrax toxin," *nature biology* 14, no. 10 (October 2001), 958-61. Relevant work of John Collier at Harvard may be accessed at <http://focus.hms.harvard.edu/2001/Oct12_2001/research_briefs. html> and of Rodney Tweten at Oklahoma State University may be accessed at <http://www.mipt.org/ouhscanthrax.asp>.

[43] In this circumstance, antitoxin treatment could be an interim solution, until a vaccination took hold.

[44] In effect, a vaccine does not confer complete immunity but rather raises the LD_{50} (the infectious dose that is anticipated to be fatal for 50 percent of the population) to a much higher level.

[45] In the longer term, other methods, some now supported in their early stages by DARPA and NIAID, may provide other mechanisms of protection, such as attacking anthrax spores in the lungs.

[46] It is also sometimes called *detect to protect*. I will use *detect to warn* to encompass both phrases.

[47] The human lung is a concentrator for some potent biological agents. As a result, small atmospheric concentrations can unfortunately have large effects in the human body.

[48] It would also be on the order of 1 in 10,000,000,000 that five consecutive tests failed to detect the attack, unless the system suffered from a systemic problem (for example, if it did not test for the agent in question or if the agent did not pass through detectors).

[49] The following commentary describes what would happen "on average" and ignores fractions of hours for clarity.

[50] Put another way, when an alarm sounded, there would only be a 1 in 18 chance-less than a 6 percent probability-that an

attack had occurred. In practice, the matter would not be quite this simple. The continuous (or discontinuous) nature of the alarms could affect reactions. On the one hand, since (by hypothesis) the 5 accurate alarms (true positives) would arise in the context of 1 continuous attack, there would be 87 false positives for each (5-hour) attack. On the other hand, a decision-maker could bring the effects of the false positive rate down by sounding an alarm only after two consecutive positive tests. This, in turn, would mean that the population would be exposed for an additional hour during an attack.

[51] Or, following the logic of the preceding footnote, there would be on average more than 870 false positives for each real attack.

[52] The differentiating markers are whether they contain tryptophan or other fluorescent biomolecules.

[53] This assessment is drawn from discussion with the staff of the Department of Defense Joint Program Office for Chemical and Biological Defense and is based on their urban field experience over the last 12 months. This experience is invaluable. A detector system cannot simply be installed, turned on, and operated at a predictable false positive level. There are great geographic, seasonal, and diurnal variations in the atmospheric biology of American cities. Just as the U.S. Navy understands that its submarine sonar detection systems can only be operated effectively against the backdrop of careful studies of the water and terrain, so, too, installed detector systems may need to operate for at least one year in order adequately to document background conditions (the *detector environment* or, to use a more technical term, the *ecotone*). Furthermore, field experience is required to determine the effects on the instrument of maintenance, resupply, deterioration, repair and operator error. Unfortunately, even extended field experience is a fallible guide to false positive rates. Conditions can change, not only naturally but also as a result of terrorist actions, such as using explosives alongside of biological weapons (increasing fire, smoke, dust, and other contaminants) or by the concomitant release of agents designed to be misleading or by masking the signature of actual agents.

[54] Lawrence Livermore National Laboratory has developed a method for accelerating polymerase chain reaction (PCR) tests that can bring test times down to two hours for a range of agents. This system is being applied to a new "biowatch program," using EPA collectors in selected cities. It is not, however, yet linked to a local laboratory system. In practice, therefore, it takes considerably longer than the six hours associated with other systems and described in the text. Direct nucleic acid-based detection technologies offer an alternative possible rapid approach. They would permit future agent identification without PCR amplification.

[55] DOD has requested a certification to this effect from the Food and Drug Administration, but a due course determination on this point is expected to take years. Accelerating this process could be very valuable.

[56] For plague, it takes 72 hours.

[57] As implied by the above, the process is more complicated and more extended for toxins and viral agents.

[58] Or in times of tension or particular vulnerability.

[59] We may also be willing to accept more false positives for some agents than for others. Those charged with acquiring and deploying radar systems have developed analogous judgments about trade-offs between desirable increases in sensitivity and undesirable increases in false positives. These are described as "receiver operating characteristics." A very lucid introductory account of this subject, applied to medical diagnosis, may be accessed at <http://www.anaesthetist.com/mnm/stats/roc>. I am indebted to Timothy Coffey for referring me to this Web site.

[60] This will be all the more likely if threats present themselves that are essentially untreatable. If a hemorrhagic fever, for example, were weaponized, detect to treat would not be a viable strategy because we have no meaningful treatment. By contrast, in a heightened alert posture, populations at some distance downwind could benefit from a strategy of detect to warn. When warned, they could stay indoors with ventilation systems turned off. (Most commercial systems can be set to recirculate indoor air.) As long as 40 years ago, it was noted that even crude methods of self-help can yield real benefit. "A man's cotton handkerchief, when folded to a thickness of sixteen layers, proved 94 percent respiratory protection . . . when crumpled it provided 88 percent protection. . . . [A] bath towel folded in two layers provided 85 percent protection. It was found, however, that the high resistance of the handkerchief, when folded to 16 layers and when crumpled, limited the usage of these two variations to short intervals." See U.S. Army Chemical Corps Biological Laboratories, "Technical Manuscript 3: Physical Protection from Biological Aerosols" (Fort Detrick, MD: April 1962). Reproduced by the Armed Services Technical Information Agency as AD 279 888. A more refined system of civilian protection (involving, for instance, HEPA or other improved filters, masks, public education) could amplify the benefits of warning. The general topic is identified under the heading "Citizen Protection" below.

[61] Clarifying this point will itself be helpful. Similarly, though mayors, governors, and local first responders have essential roles to play in the wake of an attack, it is doubtful that it is useful to invest local officials with the authority to decide or announce that an attack has occurred. To avoid intolerable inconsistency and alarm, a single Federal authority should be expected to make this national security judgment. This underscores the importance of the Federal role discussed in the context of Recommendation 4.

[62] "A bioweaponeer will know to strike at dusk," states a leading former Soviet biological weapons developer. See Ken Alibek, *Biohasard* (New York: Random House, 1999), 21.

Induction is most common at this time of day. Night is also the time when an agent is least exposed to ultraviolet rays. *B. anthracis* is less vulnerable to sunlight than many agents because it forms a robust spore. But even this agent degrades significantly in sunlight.

[63] The recently announced "biowatch system" intended to protect cities through use of existing EPA samplers collects samples at twenty-four hour intervals.

[64] In this circumstance, other rarely discussed considerations become relevant, such as how to protect installed devices, their mean time between failure, and maintenance and repair costs.

[65] This is not to say that detectors would have no value in a civilian anthrax attack. They may help us to ascertain where and how an attack occurred and, thereby, to ascertain areas of exposure and to identify the attacker modus operandi and perhaps identity. They can help alert us not only to evacuate particular facilities but also to sensitize medical and law enforcement systems to the possibility that an attack has occurred.

[66] This proposition is debatable—and it would be valuable to have the debate and reach a consensus result among expert

advisors. Many generalizations about inhalational anthrax are derived from monkey studies, whose applicability to human beings may be imperfect. In the only mass human experience, the 1979 accidental release of anthrax from a Soviet weapons facility in Sverdlovsk, data is difficult to establish (the Soviet Union had an interest in suppressing information), and, most probably, the anthrax release was small. For planning purposes, this paper assumes that a terrorist aerosol dispersion of anthrax would involve a substantial quantity of agent (at least several kilograms) and that among the many infected, a significant number would have vulnerabilities that would cause them to rather quickly manifest the symptoms of the disease.

[67] The presence of Gram-positive staining bacteria in a patient who was healthy 2 days previously is a clear indication of anthrax. Only a small percentage of patients will develop the illness within 24 to 36 hours, and only some of these will have *B. anthracis* in their blood in sufficient quantities to be visible by staining within 4 hours. But in an aerosol attack, the numbers of those exposed will be so large, and those close to the source of dissemination are likely to be hyper-exposed, so that a subset of the population can be expected to present as markers. Later in the illness, an X-ray showing a widened mediastinum will be a clear clinical indication of anthrax. The RSVP on-line surveillance system developed at Sandia National Laboratories and implemented in some American jurisdictions uses this as a principal indicator of an anthrax incident. But this clinical symptom is not likely to be evident until at least the third day after infection. Before that time, RSVP and similar systems will be helpful mainly in showing the increased number and distribution of patients with influenza-type symptoms.

[68] As noted above, it is also possible that PCR amplification can br rendered unnecessary by direct nucleic acid evaluation.

[69] See generally Donald A. Henderson et al., "Smallpox as a Biological Weapon: Medical and Public Health Management," *Journal of the American Medical Association* 281 (June 9, 1999), 2127–2137, and Tara O'Toole, "Smallpox: An Attack Scenario," *Emerging Infectious Disease* 5 (1999), 540–546.

[70] In natural outbreaks, the ring strategy (sometimes called a trace strategy) calls for tracing and vaccinating those in "a ring" around infectious carriers of the disease (that is, those who had close contact with a carrier). In an aerosol case, the analogy to that strategy would be to identify those in the area under the aerosol cloud and vaccinating them.

[71] For example, Christian Scientists.

[72] No national program can be identified in which we have ever achieved as much as 98 percent compliance. Accordingly, at least six million Americans can be expected to have avoided inoculation.

[73] Unfortunately, the scientific evidence on this point is limited. Sooner vaccination is always better than later and susceptibility to the disease will vary with the magnitude of infection, the virulence of the strain, the health of the infected individual, etc. The 96th hour is a rough marker of the point before which it can be presumed that vaccination will be effective and after which it is likely to be ineffective. But the marker should not be taken to be a rigid boundary. The evidence and the inference to be drawn about post-exposure smallpox vaccination is well discussed in a section of the University of Minnesota Center for Infectious Disease Web site, accessed at <http://www.umn.edu/cidrap/content/bt/smallpox/biofacts/smllpx-summary.html#_Use_of_Vaccine_2>. The fact that in the event of exposure, earlier vaccination is more protective than later vaccination will make it especially difficult to manage a vaccination program for an exposed population. It also argues powerfully for permitting citizens the opportunity to choose vaccination prior to attack. Even if we can and do vaccinate everyone exposed to an aerosol attack, those who are vaccinated with more delay after an attack will be at greater risk than those vaccinated earlier. This consequence will be especially intolerable and difficult to justify if it follows upon a decision to deny Americans the opportunity for pre-attack vaccination. Before broad pre-attack vaccination would be permitted, however, it is still necessary to weigh the likelihood of a smallpox aerosol attack against the likely costs of vaccination.

[74] See James W. LeDuc et al., "Smallpox Research Activities: U.S. Interagency Collaboration, 2001," accessed at <http://www.cdc.gov/ncidod/eid/vol8no7/02-0032.htm>. This Web site from the Centers for Disease Control, Emerging Infectious Diseases, identifies work on more than 20 antiviral drugs, but only cidofovir has reached the stage of being an investigational drug.

[75] This is especially so because, while anthrax may require on the order of 10,000 bacteria to kill a typical person, the average lethal dose for smallpox may be only one virion. The boundaries of a lethal area for aerosol smallpox are therefore likely to be both more difficult to detect and more difficult to define.

[76] These plans also need to address strategies for isolation and support of those who are unable or unwilling to be vaccinated. For immune-compromised individuals, *vaccinia* (the attenuated smallpox virus used for vaccination) can be nearly as dangerous as smallpox itself. Accordingly, it is likely to be desirable to isolate these individuals (probably in their own homes) and to sustain them with services from individuals who were vaccinated some time previously. It should be noted that the existence of such a system would not obviate the risk from attacks on rural or other areas without deployed detectors.

[77] See LeDuc et al.

[78] If also effective during the period between the fifth day of infection and the time of appearance of symptoms (usually around the twelfth day), it could also be a trigger for the administration of antiviral drugs as these are developed. Anthony Fauci, Director of the National Institute for Allergic and Infectious Diseases, has been making this point for some time. It appears that his position is complementary to the one advanced in this paper.

[79] However, the timing of pre-attack mass vaccination may still be an issue. If a safer vaccine can be developed and tested within a few years, it may be worth deferring vaccination. Furthermore, if vaccination is initiated, it can and should proceed incrementally. A small population of ten to twenty thousand first responders can be vaccinated, the resulting complications observed and measured, and then a second larger cohort can be vaccinated and observed. If the program has minimal complications, vaccination can be offered to ever-larger segments of the population. It would be prudent, however, not to offer mass vaccination in advance of the relevant data. See also Joshua Epstein et al., "Toward a Containment Strategy for Smallpox Bioterror: An Individual Based Computational Approach," Working Paper 31 (The Brookings Institution-Johns Hopkins University Center on Social and Economic Dynamics, December 2002), 14. The detailed mathematical modeling underlying this paper does not, however, deal with a large aerosol attack.

[80] This capability must include not only the ability to develop, test, and stockpile the relevant drugs and vaccines, but also, as illustrated by the cases analyzed above, to distribute these drugs and vaccines in a timely manner. Lawrence Wein, Donald Kraft and Edward Kaplan, have powerfully highlighted the rewards of timely distribution in their admirably precise mathematical analysis of an anthrax attack rather like "Case One." See their article, "Emergency Response to an Anthrax Attack," PNAS (April 1, 2003), vol. 100, number 7, pp 4346–51. See also their parallel analysis of a smallpox attack rather like "Case 2," Kaplan et al, "Emergency Response to a Smallpox Attack: The Case for Mass Vaccination" PNAS (August 6, 2002), vol. 99, no. 16, 10035–40.

[81] Mass decontamination is an orphan issue. Though several agencies and many contractors have relevant programs and products, no Federal agency has assumed responsibility for more than pilot programs or single building, small area decontamination problems. The Environmental Protection Agency has relevant experience from superfund sites and has, through its Office of Pesticide Programs, sponsored at least one "interagency working meeting" on the subject (see <http://208.184.25.73/biothreats/mtg/index.htm>), but it has only a half dozen emergency response teams and is not positioned to assume operational responsibility for an urban crisis. The Department of Homeland Security sponsors some research in national laboratories on decontamination, but these are not close to the mass application that would be required in the Cases described here. DARPA has supported research that contributed to the decontamination of the Hart Office Building. The Department of Defense has relevant experience from decontaminating its laboratories. But DOD is not significantly focused on the problem because it does not see decontamination of U.S. urban areas as a part of its mission, and decontamination of battlefields is not a wartime priority. The aerosol anthrax case focuses attention on the fact that all of Manhattan could be covered in anthrax, with grave repercussions for our national economy as well as for those living and working there. In this context, standards of complete decontamination (such as those applied to the Hart Office Building) are not likely to be sustainable. But what are acceptable lesser standards? A decision in advance would spare us a distracting and divisive debate after an attack and would facilitate investment in the relevant technologies. In December 2001, the Centers for Disease Control and Prevention and the National Center for Infectious Diseases cosponsored a valuable meeting on "*Bacillus anthracis* Bioterrorism Research Priorities for Public Health." That meeting briefly touched on this point, recommending (but not funding!) background studies as "a secondary objective" of "Working Group 3's" second research priority. See page 14 of the "Meeting Notes." The point is more important than that, though it was understandably less salient to a group focused on "public health," rather than decontamination. If we cannot effectively perform large-area decontamination, we are inviting critical asset attack.

[82] Interdiction is the act of preventing a perpetrator from attacking. Recognition of the likelihood of reload highlights the importance of this capability. The FBI and our intelligence agencies need to plan for the steps that might be taken to thwart later attacks after a first attack. This concern must be addressed separately from (though it is intimately related to) intelligence, attribution, and the collection of evidence leading to the identification and successful prosecution of a perpetrator. At a minimum we should focus on developing a rapid ability to assess the modus operandi as well as the agent associated with the initial attack and to deploy law enforcement efforts accordingly.

[83] The threat of bioterrorism warrants the development of special collection priorities, analytic efforts, and indicators and warnings.

[84] As used here, *surveillance* refers to the collection and analysis of health data from patient populations, pharmacy use, groups identified as "health sentinels," animal or plant specimens, etc. Human surveillance has become more robust in recent years through the evolution of ESSENCE (used by the Department of Defense), RSVP, and several municipal systems. In regard to the latter, see, for example, Richard Perez-Pena, "System in New York for Early Warning of Disease Patterns," *The New York Times*, April 4, 2003, A1.

[85] Simulation and gaming are particularly important because we have so little experience with bioterrorism. When analogous natural outbreaks have occurred, they have typically been under circumstances and in populations that are significantly different from our current situation. Implicit or explicit expectations about the responses of bureaucratic systems, our population at large, and our terrorist opponents underlie many of our planning premises, but need to be illuminated and tested by "red-teaming" and by table top and larger exercises. Mathematical models of agent dissemination, contagious infection, and other variables are also prerequisite for good planning and good response.

[86] Issues within this area include whether and how biological knowledge should be classified, how to limit the proliferation of Russian and other biological warfare expertise, and how, if at all, cross-border movements of biological materials could be regulated or at least observed. The National Academy of Sciences has been a leader of work in this area.

[87] This involves citizen education, physical protection (for example, filters or masks), building protection, psychological preparation, and other similar measures. Little effort is now expended on these important subjects. No Government agency has made the development of this set of capabilities a central mission. Hopefully, the Department of Homeland Security will correct this oversight. Private contractors have little financial incentive to operate in this area. The Alfred P. Sloan Foundation, the Red Cross, and the Center for Technology and National Security Policy at the National Defense University have each commendably initiated work on citizen education, but they are limited in the resources that they can bring to bear. The Century Foundation has focused on improving and analyzing media understanding of bioterrorism and government relations to it. See particularly, Patricia Thomas, *The Anthrax Attacks* (New York: The Century Foundation, 2003), accessed at <http://www.tcf.org/Publications/Homeland_Security/thomas_anthrax.pdf>. See also, Nancy Ethiel, "Terrorism, Informing the Public" (Chicago: McCormick Tribune Foundation, Cantingy Conference Series, Conference Report, 2002). It is imperative that Federal agencies develop better coordination among themselves as to public statements that will be made in a biological emergency, and then expand this understanding to embrace state, local, and private spokespeople who will inevitably offer advice and analysis in the wake of a biological attack. DARPA and the interagency Technical Support Working Group (both reporting to DOD) have each initiated some research and demonstration activity designed to organize filtration and other systems to achieve what DARPA describes as "an

immune building." By Congressional direction, the EPA is initiating a "safe building program."

[88] This is a very large, demanding, and critical set of capabilities. Subtopics would include issues such as the ability of our health care system (which, for economic reasons, normally operates very close to capacity) to respond to widespread catastrophic events; our ability to maintain law and order; our ability to sustain systems of transport and supply of medicines and mundane items like food; our capabilities for obtaining and retaining situational awareness; and our mechanisms for disseminating information and advice in circumstances of confusion, multiplicity of state, local and Federal officials, etc. All DISC capabilities raise issues about the roles and missions of our Federal, state, and local bureaucracies. But this set of capabilities raises these issues more severely than any other. A useful conceptual framework for this topic is provided by the Army Office of the Surgeon General in its publications "Understanding and Application of the Chemical, Biological, Radiological, and Nuclear (CBRN) Analytical Framework" and in "Commanders' Guide for CBRN Events." Drawing upon the World Association of Disaster and Emergency Medicine guidelines, these publications define the consequence management problem in terms of a five-point cycle. The points that warrant attention are: a hazard (or vulnerability), an event, resulting damage, impacts from that damage, and a resulting situation. Effective consequence management requires five corresponding interventions between these points in the cycle: planning (with respect to known hazards), preparedness (for anticipated events), mitigation (for events that have occurred or are occurring), response (to damage), and recovery (from impact). Any or all of these five actions will in turn affect the resulting situation.

[89] The Defense Science Board has prepared a stoplight chart to the same effect with regard to our progress, and likely progress over the next decade, with vaccines, therapeutics and diagnostics for nineteen anticipated threats.

[90] See, for example, note 18, above.

Appendix: Acknowledgments and List of Experts Consulted

I found the following noted individuals to be particularly helpful in the course of my preparing this paper. None of these people are responsible for my errors and judgments. All, however, made this paper—and in their everyday work are making the nation's defense against bioterrorism—better.

Amy Alving (Defense Advanced Research Projects Agency), Steve Arnon (California Department of Health Services), Michael Ascher (Department of Health and Human Services), Beverly Berger (Department of Energy), Kenneth Bernard (Department of Health and Human Services), Peter Biggins (Porton Down), Roger Breeze (Department of Agriculture), Todd Brethauer (The Technical Support Working Group), Roger Brent (The Molecular Sciences Institute, Berkeley, California), Lisa Bronson (Office of the Secretary of Defense), Robert Buchanan (Food and Drug Administration), Michael V. Callahan (Massachusetts General Hospital and Center for International Health, Boston University School of Public Health), Thomas Carey (Federal Bureau of Investigation), Seth Carus (National Defense University), Jerry Conley (Defense Threat Reduction Agency), Ruth David (ANSER), Jerry Donlon (Department of Health and Human Services), Millie Donlon (Defense Advanced Research Projects Agency), Gerald L. Epstein (Defense Threat Reduction Agency), Anthony S. Fauci (National Institute of Allergy and Infectious Diseases), David Franz (Southern Research Institute), Art Friedlander (U.S. Army Medical Research Institute of Infectious Diseases), Michael Goldblatt (Defense Advanced Research Projects Agency), Julie Gerberding (Centers for Disease Control and Prevention), Darryl Greenwood (Massachusetts Institute of Technology Lincoln Laboratory), Peggy Hamburg (Nuclear Threat Initiative), Dan Hanfling (INOVA Fairfax Hospital), Anne Harrington (Department of State), Jerry Hauer (Department of Health and Human Services), D.A. Henderson (Department of Health and Human Services), Michael Hopmeier (Unconventional Concepts, Inc.), John Humpton (Department of the Army), Noreen Hynes (Food and Drug Administration), Dave Huxsoll (Department of Agriculture), Leeanne Jackson (Food and Drug Adminstration), Tom Inglesby (Johns Hopkins Center for Civilian Biodefense Strategies), Peter Jahrling (U.S. Army Medical Research Institute of Infectious Diseases), Bernadette Johnson (Massachusetts Institute of Technology Lincoln Laboratories), Anna Johnson-Winegar (Office of the Secretary of Defense), CAPT Shaun Jones (U.S. Navy), Donald Kraemer (Food and Drug Adminstration), Andrew Krepinevitch (Center for Strategic and Budgetary Assessments), Carol Kuntz (Office of the Vice President), Diane Kotras (Office of the Secretary of Defense), Larry Lynn (Defense Science Board), Josh Lederberg (The Rockefeller University), Randy Larsen (ANSER), Marci Layton (New York City Department of Health), Terry Leighton (Children's Hospital Oakland Research Institute), Fred Leykam (The Washington Institute), Scooter Libby (Office of the Vice President), Thom Mayer (INOVA Fairfax Hospital), Michael Osterholm (University of Minnesota), Tara O'Toole (Johns Hopkins Center for Civilian Biodefense Strategies), William Patrick (Independent Consultant), Steve Reeves (Department of Defense, Joint Program

Office, Chemical and Biological Defense), David Relman (Stanford University), Dan Rock (Department of Agriculture), Phillip K. Russell (Department of Health and Human Services), Alan Rudolph (Defense Advanced Research Projects Agency), June Sellers (U.S. Army), Stuart Simonson (Department of Health and Human Services), John Vitko, Jr. (Department of Homeland Security), Steve Wax (Defense Advance Research Projects Agency), William Winkenwerder (Office of Secretary of Defense), and Al Zelicoff (Sandia National Laboratories).

In addition, I am grateful to Julie Evans, Paul Hughes, William Laster, Dannie Smith, Jerry Warner, and Jan Weaver for their invaluable administrative support, to Andrew Marshall, Director of the Office of Net Assessment, and Michael Goldblatt for funding this project, and to Hans Binnendijk of the Center for Technology and National Security Policy at the National Defense University and Anne Harrington at the National Defense University for support of a workshop with experts on detector systems.

About the Author

Richard Danzig is a consultant on bioterrorism particularly and on terrorism generally to several Department of Defense agencies. He was Secretary of the Navy from 1998–2001 and the Under Secretary of the Navy from 1993–1997. Among other activities, he is a Senior Fellow of the Center for Naval Analyses, a director of Human Genome Sciences Corporation, the National Semiconductor Corporation, and Saffron Hill Ventures, and Chairman of the Board of the Center for Strategic and Budgetary Assessments.

CENTER FOR TECHNOLOGY AND NATIONAL SECURITY POLICY
NATIONAL DEFENSE UNIVERSITY
FORT LESLEY J. McNAIR
WASHINGTON, D.C.