Title: Bioterrorism: Threat And Preparedness
Date: Spring 2002
Source: National Academy of Engineering

Abstract: Policy makers and scientists must assess the probability of threats as well as the amount of damage they might do.

Prior to the anthrax mailings that followed the terrorist attacks of September 11, much of the criticism about planning and preparedness for bioterrorism attacks had been focused on the mismatch between the assessments of the threat and the size and structure of the planned response. Many analysts had criticized plans for overemphasizing worst-case scenarios and underemphasizing more probable middle- and low-casualty attacks. Most worst-case scenarios involved the release of a military-style biological agent in aerosol form near an urban center; everyone exposed to the pathogen would become severely ill, and many would die; casualties would number in the tens or even hundreds of thousands. Scenarios involving contagious pathogens, such as smallpox or plague, were even more worrisome. Outbreaks involving such pathogens evolve over time, and unless appropriate measures are taken, the numbers infected and the size of the affected geographic area would expand exponentially.

The anthrax mailings were not the mass-casualty bioterrorism many had expected. Although the military-grade anthrax agent was highly sophisticated, it was delivered in a relatively unsophisticated way--through the mail system. As a result, there were relatively small, localized incidents that led to a limited number of illnesses and deaths. The incidents aroused significant fear and disruptions but not mass casualties. Based on these attacks, some analysts have suggested that terrorists would not be able to orchestrate mass-casualty attacks using biological weapons. Others have considered these attacks as demonstrations of terrorists' ability to acquire high-quality anthrax, thus crossing an important threshold.

Because those responsible for the mailings did acquire (whether they also manufactured the agent remains unclear) high-grade anthrax agent but did not disseminate a sufficient quantity to produce mass casualties, both arguments are correct.

The anthrax mailings brought to public attention a recurring problem in national security planning: expectations of future developments are often vastly different from what actually occurs. Therefore, rather than planning for a narrow range of least-likely, high-consequence contingencies or focusing only on additional mailborne anthrax attacks, we must plan for a variety of future incidents--including incidents that cause mass casualties and mass disruption. In fact, planning for a variety of more likely, middle- to low-casualty incidents, while simultaneously being prepared for low-probability, high-consequence incidents is perhaps the most significant challenge facing planners. The cornerstone of preparations for future bioterrorist incidents, regardless of their nature or scope, must be a national, but not necessarily federal, public health system capable of detecting, assessing, and responding to a broad variety of contingencies.

The Challenge

Assessments of the bioterrorist threat are often either unfocused or narrowly focused on single factors. The mismatch between threat assessments and preparedness efforts can be explained partly by the failure of threat assessment methodologies to take into account all of the factors comprising the threat. Single-factor threat assessments, for example, focus either on the terrorists' motivations and objectives or on the hypothetical effects of a biological weapon, but they do not indicate which scenarios are plausible or their comparative likelihood. Consider, for example, a terrorist attack involving smallpox, which is often cited as the worst-case scenario for several reasons. First, smallpox is a highly contagious disease. Second, the population has little or no immunity to the disease. Third, even with large stockpiles of smallpox vaccine, given our highly mobile life style, it would be difficult to contain an outbreak.

We must, however, keep this threat in perspective. Despite the catastrophic effects of a smallpox attack, the probability of such an attack is extremely low, especially compared to the probability of other scenarios. First, smallpox as a naturally occurring disease has been eradicated. Second, the virus that causes smallpox is known to exist in only two high-security laboratories--one in Atlanta at the Centers for Disease Control and one at the Vector Laboratories in Siberia, Russia. Therefore, it would be extremely difficult for a terrorist to acquire the smallpox virus. Moreover, the effects of a smallpox attack would be uncontrollable and, therefore, could also affect the terrorists and their supporting constituencies. If we look at all of these factors, we must conclude that a smallpox attack is a potential contingency, even, perhaps, the most damaging potential contingency, but the probability of occurrence is very low. Nevertheless, smallpox has received the lion's share of attention and has drawn attention away from the wide range of other agents that could be used.

Rather than focusing on vulnerability to a particular organism or looking to history to determine what is to come, policy makers and scientists must recognize that the bioterrorist threat is not unidimensional. We must consider four key elements of the threat: the who (the actor), the what (the agent), the where (the target), and the how (the mode of attack). The impact of a bioterrorist attack will be determined by the interaction of these components. The more casualties bioterrorists seek to inflict, the more difficult it will be for them to assemble the necessary combination of these components. Thus, the level of risk declines as the level of desired casualties increases because the attack scenario becomes less likely.

For a number of reasons, including technical difficulties and the absence of motivation, a catastrophic bioterrorist event is not the most likely contingency. Only the release of a very contagious or very high-quality agent by a highly efficient dissemination technique could result in thousands or more casualties. In reality, the number of pathways open to terrorists that would result in catastrophic numbers of casualties are few, and those that do exist are technically difficult. The number of technical pathways for producing a low- to mid-range bioterrorism incident are more numerous, less technically challenging, and more suited to the motivations and constraints of traditional concepts of terrorism. Figure 1 (see full version of this *Bridge* issue) is a graphic representation of the bioterrorism "threat envelope." As the pyramid illustrates, the higher one moves on the casualty axis, the lower the probability of occurrence and the number of viable options. Thus, the terrorist is left with relatively few, and very challenging, contingencies for inflicting mass casualties.

Despite the low probability of a catastrophic bioterrorist attack, there is still ample cause for concern. We do not know how "massive" an attack would have to be to overwhelm the response system, instill fear and panic, or cause serious political or economic fallout. Although many terrorists will not be interested in using biological weapons or will not be able to do so, two categories of nonstate actors--those with relationships with national governments and those outside the traditional scope of governmental scrutiny--warrant particular attention. The uncertainties surrounding bioterrorism will remain, and although terrorists have yet to demonstrate the sophistication required to carry out large-scale attacks with biological weapons, the World Trade Center and Pentagon attacks have shown a willingness to inflict mass casualties. Meanwhile, the rapid development of biotechnology and the diffusion of expertise in this field may lower the technical bar over time.

Preparedness

To date, the driving factor in planning and preparedness has been meeting the threat of catastrophic casualties, without regard for its low probability. However, in our view, the relationship between the probability of occurrence and the consequences should be the basis for setting policy. Because financial resources are finite, policy makers will have to make difficult choices. Should the focus be on promoting preparedness for a single biological agent, or should we invest in measures that promote preparedness for a variety of agents and scenarios? Every dollar spent preparing for a specific agent, such as building stocks of smallpox or anthrax vaccine or purchasing antidote for botulinum toxin, is a dollar that cannot be spent on preparedness for other organisms. Given the variety of combinations among actors, agents, targets, and dissemination techniques, a public health system must be capable of rapidly and accurately detecting and assessing a large number of bioterrorism scenarios and addressing most contingencies. Rather than limiting planning and preparedness to a narrow range of catastrophic scenarios, planning should be based on developing the capability of effectively and efficiently responding to a variety of bioterrorist contingencies. In our judgment, the emphasis should be on building capacity in the public health system.

Many people assume that preparing for high-end attacks will also provide a capability of responding to middle- and low-range attacks. Consider, for example, the contents of the national pharmaceutical stockpile. In the wake of the recent anthrax attacks, the Centers for Disease Control plans to expand the national pharmaceutical stockpile and accelerate the procurement of vaccines. The bioterrorism preparedness budget currently being debated in Congress includes approximately $509 million for the procurement of smallpox vaccine, enough to vaccinate nearly every U.S. citizen. Although focusing on such high-end attack scenarios simplifies planning and preparedness by narrowing the range of contingencies, it also introduces a substantial degree of risk that the public health and medical system will be unprepared for more likely, but less drastic contingencies. Furthermore, smallpox vaccine is useless against all other agents, including anthrax, botulinum toxin, tularemia, and brucellosis. Therefore, we run the risk of neglecting other measures that could be used to meet a wide range of contingencies. We must strike a better balance between hedging our defenses against high-end, mass-casualty events and building a "system of systems" capable of addressing both a wider range of bioterrorist contingencies and natural outbreaks of infectious disease.

A System of Systems

There is no silver bullet to meet the bioterrorist challenge. Preparedness cannot be focused on a single tool for addressing the problem but must be on a system of systems that integrates a broad range of activities. The nation's public health resources--surveillance systems, epidemiological expertise, and laboratory networks--must be integrated with health care, emergency management, law enforcement systems, and others, and all of these must be connected by a system for sharing information and communicating across sectors.

Bioterrorism differs from other types of mass-casualty terrorism (e.g., chemical, radiological, or nuclear terrorism) in that it would impose heavy demands on the public health and health care systems, which would be called upon to mitigate and ameliorate the consequences of an attack and to assist the law enforcement community in gathering criminal evidence. Thus, we must build medical management capacities--including stockpiles of vaccines, antibiotics, and other supplies and systems for rapidly distributing these materials--and a system connecting the "front-end" awareness and assessment capacities to the "back-end" of the bioterrorism response system. Without robust capabilities for early detection and rapid assessment, the response to an act of bioterrorism may be ineffective or too late. As the recent anthrax incidents have shown, awareness and assessment capacities, particularly epidemiological and laboratory capacities, can be quickly overwhelmed. These capabilities, which were critical in assessing the risk of anthrax exposure, were slow to complete an assessment of risk despite knowing that an attack had occurred. The nature of future bioterrorist attacks may not be as readily apparent as the anthrax mailings have been. More covert attacks would place additional strains on the public health system to detect the attack, diagnose the agent and illness, and determine the scope of exposure and future course of the illness.

Surveillance

Early detection will be critical to saving lives. The sooner a bioterrorist event is detected, the sooner an assessment of the event can be completed, and the sooner medical care can be administered to those exposed. In the case of contagious diseases such as smallpox or pneumonic plague, detecting an outbreak early is essential to containing the outbreak. People today are incredibly mobile, commuting in and out of urban centers on a daily basis and traveling all over the world regularly. Failure to detect an outbreak of a contagious disease early could result in its rapid spread.

A national surveillance system to provide an early warning of unusual outbreaks of disease, both natural and intentional, will be a critical component of our preparedness. This system will depend on an information infrastructure that includes electronic data networks connecting local public health departments and area health care providers and providing regular analyses of the data for the presence of unusual trends that could indicate a bioterrorist attack. Additional sources of data that could provide an early indication of a bioterrorist attack include spikes in flu-like symptoms, over-the-counter drug sales, or absenteeism. The crucial element will be a robust information infrastructure for collecting, analyzing, and sharing information from all of these sources.

Epidemiology

Epidemiologists play an important role in surveillance and detection. They routinely monitor disease trends and take appropriate measures to meet potential public health threats. Epidemiologists will also be critical in determining the scope of the exposure to a bioterrorist agent once it has been detected. Typically, they trace the outbreak back to its source, determine who was in the exposed area at the time of release, and recommend medical management measures. Because of the labor-intensive nature of epidemiology, which depends largely on interviews and analyses of disease trends, state departments of health will have to hire and train staff to be aware of natural outbreaks of disease as well as the wide range of bioterrorist agents.

Laboratory Requirements

Public health laboratories also play a critical role in the detection and assessment of bioterrorist incidents. A spike in requests for culture analyses from physicians could indicate an unusual outbreak of disease. Once an attack has been detected, laboratories will be critical in identifying the biological agent released. During the anthrax mailings, laboratories were called upon to determine which people in the proximity of the contaminated mail had been exposed and to assist law enforcement in gathering forensic evidence for prosecuting the perpetrator(s). Upgrading laboratory capac-ity by expanding advanced diagnostic capabilities, increasing the range of bioterrorist agents that can be identified at state and local laboratories, and making diagnostic exams faster and more accurate will be critical to an effective preparedness system.

Information and Communication

The underpinning for all of the components of an integrated detection, assessment, and response system will be a robust information infrastructure. Surveillance, epidemiology, and laboratory capacities for meeting the bioterrorist challenge will all depend on a robust information infrastructure. Information technology could be used to exchange procedural guidelines prior to a bioterrorist event, provide a mechanism for compiling and analyzing data on disease trends from different sources, share information during an event and lessons learned after an event, and provide training for all constituencies. In addition, accurate and timely information will be the backbone of the decision making process in times of crisis and will provide credible and consistent information to the general public to reduce panic. Bolstering and integrating existing information infrastructures to respond to bioterrorism will require expanding our technological infrastructure, as well as improving human and social understanding of how the infrastructure can be most effective.

Building Response Capacities

Any response system must have built-in flexibility so it can respond appropriately to a large-scale or small-scale event. Flexibility will require effective awareness and assessment tools that provide information on the nature of the attack so the response can be tailored appropriately. Local and federal responses should be based on a tiered, scalable approach commensurate with the scale of the attack.

Conclusions

Building and sustaining the public health system of systems described here will require sustained investment in people, technology, and materials. Adequate numbers of trained public health and medical personnel will be necessary to monitor the nation’s health on an ongoing basis, operate and maintain the network of public health laboratories, investigate and analyze unusual outbreaks of disease, and provide preventive and therapeutic medical care for natural and intentional outbreaks. Building this system will also require investments in several key technologies, including the technologies for an electronic information infrastructure that can link federal, state, and local public health departments, hospitals, clinics, physicians’ offices, and other medical care providers into a national public health network. Other technologies will be necessary to increase the speed and throughput of public health laboratories. An effective system of systems will also require adequate stocks of antibiotics, vaccines, and medical supplies--at both the national and local levels--to ensure that adequate treatment is available.

Creating and sustaining investments in people, technology, and materials will require strong partnerships between federal, state, and local governments, each of which will provide key capabilities in the public health system of systems. The role of the federal government will be to provide funding to support local and state preparedness and to take the lead as system integrator. A strong partnership between the public and private sectors--especially private health care institutions like hospitals and private-practice physicians--will also be important. The private sector should play a role, although the private sector cannot be expected to assist in planning for the mass distribution of medications or to maintain surge capacities for unlikely contingencies. That task will fall to state and local governments (National Academy of Engineering, 2002).