# Bio Terror Bible

## EXPOSING THE COMING BIO-TERROR PANDEMIC

**BIOTERRORBIBLE.COM:** The following whitepapers were published by think-tanks, universities, NGO's and various governmental agencies and have at the very minimum set the stage psychologically for the impending bio-terror induced pandemic. The simple fact that these whitepapers exists in mass confirms that an upcoming bio-terror attack is in the cards and may be played in a last ditch effort to regain political, economic and militarial control of society.

**WHITEPAPERS:** Army War College , ASM (American Society for Microbiology), CATO Institute, Center for a New American Security, Center for Biosecurity of UPMC, Center for Counterproliferation Research, Chemical and Biological Arms Control Institute, CRS (Report for Congress), GAO (General Accounting Office), Institute for National Strategic Studies, Institute for Science and Public Policy, Johns Hopkins University, National Academy Of Engineering, National Defence University, PERI (Public Entity Risk Institute), RIS (Research & Information System), Terrorism Intelligence Centre, The Federalist Society, UNESCO (United Nations), University of Laussane, and the WMD Center.

**Title:** Biological Terrorism In The United States: Threat Preparedness And Response: Final Report
**Date:** November, 2000
**Source:** Chemical and Biological Arms Control Institute

**Abstract:** Over the last several years, a confluence of events – the World Trade Center bombing, the Tokyo subway sarin gas attack by the Aum Shinrikyo, and the bombing of the Murrah Federal Building in Oklahoma City – focused attention on the growing threat of terrorist use of chemical, biological, radiological, or nuclear (CBRN) weapons in the United States. These developments gave rise to a set of perceptions – among policy makers and the public alike – that the United States is vulnerable to terrorist attack; that such attacks could entail the use of CBRN weapons; and that the United States has not been well prepared to deal effectively with such a challenge. Biological terrorism differs from other types of CBRN terrorism in that it would impose particularly heavy demands on the nation's public health and health care systems. Although a chemical attack would also tax these systems, bioterrorism would impose especially stressful burdens. Yet, that same public health system is the crucial factor in an effective response.

A highly effective public health system should make an important contribution to deterring the threat by demonstrably diminishing the gains of a potential attack. It also constitutes the "first line of defense" in the event deterrence or prevention fails. Ultimately, it will be the public health system that will be called on to mitigate and ameliorate the consequences of a terrorist attack using biological weapons. A number of programs are underway to improve the health and medical dimensions of the national response to the threat of bioterrorism. Uncertainty exists, however, as to whether current programs are those that are most needed or whether they are being implemented in the most effective way possible. This uncertainty exists because to date there have been insufficient means to judge the efficacy of existing programs. This lack of criteria is the product of not having an analytic framework that establishes national requirements for an effective response derived from a comprehensive threat assessment. The development and application of a strategic framework is urgently needed. Making a contribution to the development of that framework is the purpose of this project.

## Conclusions & Recommendations

This Part offers conclusions and recommendations based on the assessment of the bioterrorism threat and its relationship to the function and organization of preparedness and response efforts. In addition to the specific recommendations related to each of the functional areas discussed in Section I of Part III, this discussion formulates a series of general recommendations on the HHS's and CDC's bioterrorism preparedness program based on how the nature of the threat shapes each function in an integrated bioterrorism detection, assessment, and response system.

For a number of reasons, including technical difficulties and motivational issues, a catastrophic bioterrorism event is not the most likely contingency U.S. officials and the American people will confront. The number of technical pathways available for achieving a catastrophic bioterrorism incident is limited.

The technical pathways for producing a low to mid-range bioterrorism incident, however, are more numerous, less technically challenging, and fit better within the motivations and constraints of more traditional concepts of terrorism. Figure 3 shows a graphic representation. At the top of the pyramid rests the narrow set of high-consequence, low-probability bioterrorism attacks. Moving down the pyramid, the likelihood of attack increases, the severity of consequences decreases, and the number of technical pathways increases.

This threat analysis shapes the nature of the public health and medical response at a number of key points. The first issue is which segment of the pyramid is the basis for HHS and CDC planning and preparedness. Today, the answer seems to be the top section in which the driving factor is the potential of some agents to create catastrophic casualties even though such scenarios are less probable than other types of incidents. It is assumed that preparing for the high-end attacks provides a capability to respond to the middle and low range attacks. But in certain areas, this assumption does not necessarily hold true.

**Examples include:**

**1.** Providing doctors and nurses with only the training to recognize and treat the list of top three or four agents defined by their casualty potential;
**2.** Conducting training, and providing protocols and reagents for a limited set of threat agents to laboratories;
**3.** Developing the National Pharmaceutical Stockpile based on the treatment and prophylaxis requirements for a large-scale attack using the most lethal agents, including large expenditures of resources on stockpiling large quantities of smallpox vaccine; and
**4.** Drafting local-area response plans with a focus on massive response capability with little attention provided to responding to low or middle range attacks.

Focusing planning and preparedness on the set of high-end attack scenarios may simplify planning and preparedness efforts by narrowing the range of types of scenarios against which a capability should be developing. But, as the examples listed above begin to demonstrate, preparing for the high-end attacks provides some level of preparedness against a narrow set of contingencies at the risk of being unprepared for the most likely scenarios, or inappropriately responding to a low or middle range incident in a massive fashion. Such a response could produce the severe social disruption and psychological impact many terrorists look to achieve. The low probability of "catastrophic" bioterrorist events, however, is no reason for complacency. Events that produce lower levels of casualties, which are far more likely, will also stress response systems severely, particularly at the local level. Moreover, the psychological impact of any attack is hard to estimate, and it could be profound.

### The Need for Flexibility

This analysis suggests that HHS and CDC must shift their planning assumptions from an emphasis on preparedness for the narrow set of high-end bioterrorism incidents to preparedness for the wider array of low and middle-range attacks while hedging against the possibility of a high-end attack. This shift in

emphasis entails improving the nation's public health and medical system in such a way as to promote robust awareness and assessment tools as well as flexibility within the response system. Robust awareness capabilities will increase the likelihood of early detection; effective assessment tools allow for proper characterization of the event; and flexibility gives the system the ability to react to incidents according to their actual nature. Emphasizing flexibility imposes the need to alter planning and programmatic activities in a number of areas. Greater emphasis, for example, should be placed on developing response systems that are flexible and scalable according to the nature of the agent utilized and the number of people affected. Scalable response capability provides the ability to tailor the type and size of response to the type and size of attack. Importantly, increased flexibility and scalability allows the response to change over time as the event unfolds.

Improving flexibility and scalability requires execution of a number of specific planning and preparedness initiatives. Local and federal response plans should take a tiered approach that links a range of casualty figures with certain actions. Specific response capabilities should also be constructed along the basis of this tiered approach. Local response capabilities should be bolstered to be capable of responding to a certain level of casualties with a combination of regular treatment capabilities and the establishment of secondary treatment mechanisms when regular capabilities become overwhelmed. Flexibility and scalability should also be built into state and federal assistance capabilities for those incidents that overwhelm local capacity require additional assistance.

Increasing flexibility increases the demand for effective detection and assessment tools. Such robust tools facilitate early and effective intervention. Early detection and intervention decreases the burden placed on response capabilities by increasing the effectiveness of prophylaxis while simultaneously decreasing treatment requirements. Robust assessment tools provide the ability to tailor the response to the incident by identifying the agent utilized and the group of people who are likely to have been affected by the incident. Without these tools, it is impossible to assess the nature of a bioterrorism incident and impossible to calibrate the response to the attack. In situations in which detection and assessment capabilities are weak, all bioterrorism incidents are likely to be treated as high consequence incidents if they are detected at all to eliminate the possibility of some potential victims having not been provided with appropriate care.

Promoting flexibility and scalability will enhance the ability to deal with tensions inherent in the current system between the need to initiate treatment and prophylaxis as quickly as possible and the need to know the nature and extent of an attack before mobilizing a massive response. Thresholds need to be built into the bioterrorism response system to avoid a massive response to a limited, localized incident, especially given that the most likely bioterrorist contingencies are likely to produce casualty levels that do not require mass prophylaxis or treatment. Because a smaller-scale bioterrorism attack may be indistinguishable from a largescale attack early on, however, giving priority to assessment tools is essential to determining the scope of a bioterrorism attack to guide a response that is proportional. Without these tools, officials will be prone in an atmosphere of uncertainty to initiate mass prophylaxis just to be on safe side.

A three-part response system might be contemplated to achieve flexibility and scalability. The first inclination of a suspicious outbreak should trigger an initial response phase and should alert hospitals and physicians and other response personnel, require doctors to take culture samples, seek laboratory diagnosis, and notify the appropriate federal, state, and local authorities. It should also mobilize all available assessment tools, including federal assessment assets, to characterize the nature of the attack and identify available medical resources. A mobilization response may be needed when larger numbers (approaching 100 or more) of patients present, or when awareness and assessment tools indicate that an attack was fairly substantial. At this point, medical resources may need to be transported to care facilities that are receiving the bulk of patients and limited prophylaxis and treatment options may be exercised in localized areas where the attack is suspected. A large-scale response should be initiated when it becomes apparent that the attack is widespread. Considering the current nature of the bioterrorism threat, staggered response thresholds are necessary to ensure that the system does not overreact to what is most likely to be a lower-impact attack.

Another example of improving flexibility and scalability is the design of the National Pharmaceutical Stockpile. The eight push packages are uniform in size, contents, and design. In lower-consequence, higher-probability incidents, the whole push package will be deployed, but it is unlikely that everything, or even most things in it will be needed. The resulting waste is not only expensive but could leave the country open to additional attacks. One approach would be to make the individual packages more modular, allowing them to be tailored to the type of incident, but this may increase deployment times to unacceptable levels. The other approach is to maintain uniformity among the packages, but further subdivide them into a larger number of smaller packages. This approach could increase the scalability of the amount of medicines and equipment deployed to an incident while decreasing transit time.

**The Importance of Information and Communication**

Flexibility depends in large measure upon providing the right people with the right information at the right time. A robust information infrastructure underpins all of the components of an effective response system. Surveillance, epidemiology, and laboratory capacity depend on information infrastructure both in terms of capacity building -- training, networking, sharing ideas and lessons learned, and development and exchange of procedural guidelines -- and day-to-day execution. Coordinating the providers, materials, and recipients during the response to a bioterrorism incident requires robust information and communication infrastructure. Importantly, integrating detection, assessment, and response components into a system depends on developing the necessary social and technological information infrastructure to provide accurate information in a timely manner. Tightening the integration between the detection, assessment, and response will increase the system's capability to detect and assess bioterrorism incidents and then calibrate the response according the assessment.

**The Value of Public-Private Partnerships**

Accomplishing many of these objectives will require cooperation between the public and private sectors. There are key preparedness activities in which the private sector should play a role, but other preparedness activities should not burden the private sector, especially those that are only relevant in the event of a massive response to a large-scale attack. At present, the threat of a large-scale attack is low, and asking the private sector to assist in preparing massive distribution plans for medications or to maintain unnecessary surge capacities for this contingency is unreasonable.

On the other hand, there are key preparedness activities from which the participation of the private sector would greatly benefit. Surveillance is one area in which the private sector should become more involved. Health Maintenance Organizations should be encouraged to permit physicians to request laboratory culture analyses on a more routine basis, but HMO's cannot be expected to pay for hospitals to maintain surge capacities to absorb casualties from a large-scale bioterrorist attack. Likewise, private laboratories and hospitals, work places, pharmacies, etc. have a wealth of data to provide a surveillance system, and the more data sources that are integrated into the surveillance system, the better public health awareness will be. Given that surveillance is critical for providing the overarching response system with awareness, private sector participation in surveilling should be encouraged over participation in response measures that will only apply in a mass casualty attack.

It is these types of measures, the kinds that are flexible and relevant for dealing with the range of bioterrorist contingencies as well as natural outbreaks, that must be emphasized when building preparedness, at least initially. Having a massive capability to respond to a bioterrorist attack is not as useful at the present time as having a less robust response capability but good awareness and assessment tools that can detect an outbreak early, characterize it, and guide the response system effectively.

The time frame over which preparedness efforts are made is important to keep in mind. Not everything can be done immediately. The key question is what is given priority today and, as improvements in key sectors are made, what shifts in priorities can be contemplated. In essence, emphasis must be placed at the outset on building the "front-end" of the bioterrorism response system. As those capabilities are enhanced, efforts can then begin to focus more intensively on other capabilities, such as treatment

requirements.

Achieving a robust health and medical response capability will require the successful exploitation of all available information and tools. One item in this regard is the DoJ needs assessment.1 The data provided by the assessment is extremely comprehensive and could be very valuable as a tool for state public health departments to identify gaps in public health and medical preparedness and direct resources to their most efficient possible use. In addition, the data should be used as the basis for establishing more concrete cooperative agreements between public and private sector entities to aid one another in responding to a bioterrorist attack.

At the federal level, data from the assessments should be a used not only as a tool for determining the best allocation of resources to build bioterrorism preparedness, but also to raise awareness about the degree to which the nation's public health system has been degraded. Given a growing interest in public health on Capitol Hill, in particular the Frist-Kennedy sponsored Public Health Threats and Emergencies Act of 2000, the DoJ survey may give lawmakers some ammunition to reinvigorate public health capacity across the board. Therefore, it is important that the public health community, primarily HHS or CDC, have a central role in analyzing the public health and medical data compiled by the survey to ensure its accurate and credible interpretation.

Having identified the public health and medical requirements for responding to bioterrorism, HHS and CDC must elaborate a viable strategy – especially an "urban strategy" – for building public health and medical capacities for meeting the bioterrorism challenge. Given the nature of today's threat, a bioterrorist attack is likely to be a limited event for which local authorities will have primary operational responsibilities. Therefore, a strategy should take a "bottom up" approach that recognizes that the federal role in responding to a bioterrorist attack.

The DoJ needs assessment is a questionnaire provided to public safety and state public health departments to compile baseline data on local capacity for responding to bioterrorism. will depend on the severity of the attack, and for this reason the delineation between local, state, and federal responsibilities should be clear. The strategy should, above all, articulate how priorities and programs will be integrated into a holistic system in support of public health and tie capacity building to a timeline for achieving these objectives (Chemical and Biological Arms Control Institute, 2000).