Biodetection Architectures

Contributors:
Henry Abarbanel
Steven Block
Sidney Drell
Freeman Dyson
Robert Henderson
Steven Koonin
Nate Lewis
Roy Schwitters
Peter Weinberger
Ellen Williams

February 2003

JSR-02-330

Approved for public release, distribution unlimited.

JASON
The MITRE Corporation
7515 Colshire Drive
McLean, Virginia 22102-7508
(703) 883-6997

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
February 2003

3. REPORT TYPE AND DATES COVERED

4. TITLE AND SUBTITLE

Biodetection Architectures

5. FUNDING NUMBERS

130392021-DC

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The MITRE Corporation
JASON Program Office - W950
7515 Colshire Drive
McLean, Virginia 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

JSR-02-330

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

US Department of Energy
National Nuclear Security Administration
Washington, DC 20585

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

JSR-02-330

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

12b. DISTRIBUTION CODE

Distribution Statement A

13. ABSTRACT *(Maximum 200 words)*

JASON considered the essential components and operation of an effective strategy for homeland biodefense based on technologies that are currently available or likely to become available within the next five years. It is not realistic to undertake a nationwide, blanket deployment of biosensors. This might be done for the detection of airborne anthrax, albeit at substantial cost. However, there are many possible bioterrorism agents and many possible ways in which they can be delivered. Instead, biosensors should be deployed in a focused manner as one component of a broader biodetection architecture that also includes information derived from intelligence gathering and medical surveillance. This information should be analyzed by a team of local experts who are familiar with local vulnerabilities, high-value targets, and environmental conditions. The local analysis team also should be responsible for directing an appropriate response in the event of a bioterrorism attack. They will be guided by a pre-established ``playbook" that recommends particular responses for a particular set of circumstances, which will have been practiced and refined through staged exercises.

14. SUBJECT TERMS

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	None	SAR

Contents

1 EXECUTIVE SUMMARY 1

2 INTRODUCTION 3

2.1 Scope of the Study 3

2.2 Implications of a Blanket Defense 4

2.3 A Focused, Flexible Deployment Strategy 7

3 PROPOSAL FOR AN INTEGRATED BIODETECTION ARCHITECTURE 9

3.1 Components of the System 9

3.2 Intelligence Information 11

3.3 Medical Information 13

3.3.1 Sources of Information 13

3.3.2 Population Behavior 15

3.4 Monitoring Systems 17

3.5 Biosensor Information 19

3.5.1 Environmental Monitors 20

3.5.2 Sample Collection Devices 21

3.5.3 Rapidly-Deployable Sensors 22

3.5.4 Integrated Sensor Deployment 23

4 BIODEFENSE AT THE 2002 SALT LAKE CITY OLYMPICS 25

5 THE BIOLOGICAL DEFENSE INITIATIVE 29

6 ADDITIONAL RECOMMENDATIONS 33

6.1 Biodefense Working Group (BWG) 33

6.2 Biological Emergency Search Team (BEST) 33

6.3 Public Education 34

7 CONCLUSIONS 35

A APPENDIX 37

1 EXECUTIVE SUMMARY

JASON considered the essential components and operation of an effective strategy for homeland biodefense based on technologies that are currently available or likely to become available within the next five years. It is not realistic to undertake a nationwide, blanket deployment of biosensors. This might be done for the detection of airborne anthrax, albeit at substantial cost. However, there are many possible bioterrorism agents and many possible ways in which they can be delivered. Instead, biosensors should be deployed in a focused manner as one component of a broader biodetection architecture that also includes information derived from intelligence gathering and medical surveillance. This information should be analyzed by a team of local experts who are familiar with local vulnerabilities, high-value targets, and environmental conditions. The local analysis team also should be responsible for directing an appropriate response in the event of a bioterrorism attack. They will be guided by a pre-established "playbook" that recommends particular responses for a particular set of circumstances, which will have been practiced and refined through staged exercises.

Medical surveillance is the single most important component of a biodetection architecture. It relies on the American people as a network of 288 million mobile sensors with the capacity to self-report exposures of medical consequence to a broad range of pathogens. Systems have been devised to monitor a population for the earliest symptoms of bioterrorism-related diseases. These systems should be refined and similar systems should be developed to monitor the diagnostic and treatment period following a bioterrorism attack.

The biosensor component of a biodetection architecture should involve a flexible deployment strategy to meet evolving threats and vulnerabilities. Three different types of biosensors should be deployed: continuous environmental monitors placed at choke points, sample collection devices placed at high-value locations, and rapidly-deployable sensors delivered in response to specific threats. Information from biosensors must be integrated with intelligence and medical information to assist the local analysis team in formulating a timely and effective response.

It is essential to conduct realistic exercises of a biodetection architecture in order to assess technical capabilities and refine operational procedures. The Biological Defense Initiative being deployed in Albuquerque, New Mexico during June-November, 2002 does not meet these goals and seems to be little more than a demonstration of currently funded programs. Instead, a useful exercise should entail pre-defined tests of the system through a series of staged events. These tests will require careful planning, extensive participation by the local community, and follow-up analysis by an external panel of experts. Public education efforts are required to teach a prudent response in order to minimize the consequences of a bioterrorism attack.

2 INTRODUCTION

2.1 Scope of the Study

Over the past five years, JASON has conducted five studies pertaining to defense against biological warfare and bioterrorism. These include a 1999 study for DARPA on "Civilian Biodefense" (JSR-99-105), a 2000 study for the CIA Clandestine MASINT Operations Center on "Counter BW" (JSR-00-505), and a 2001 study for DARPA on "Biosensing" (JSR-01-100). The previous studies focused largely on technology issues. While there indeed are many important technological requirements pertaining to biodefense, JASON has become increasingly frustrated with the near-pervasive focus on biodetection gadgetry, rather than systems issues and the real-world context in which any such devices might be usefully deployed. For this reason, JASON was eager to take on the present study, sponsored by the Department of Energy National Nuclear Security Administration, pertaining to "Biodetection Architectures". Rather than trying to devise an ideal biosensor that could be used to detect any bioterrorism threat, this study considered the context in which biosensors would be employed as part of a broader strategy for homeland biodefense.

The chief questions that the study sought to address are the following:

1) What is an appropriate strategy for the deployment of biosensors, not just in a controlled setting, but in the real world?

2) How would a network of biosensors interface with the U.S. public health system?

3) What should be done to foster the development of an integrated system for civilian biodefense?

The study did not specifically consider "agrobioterrorism", that is, bioterrorism directed against crops or livestock. This is an important concern that could have devastating social and economic consequences. It was considered in the 1999 JASON report on "Civilian Biodefense" (JSR-99-105), and in a recent report from the National Research Council entitled "Countering Agricultural Bioterrorism" (The National Academies Press, Washington, D.C., 2002). While many issues pertaining to agricultural bioterrorism are similar to those for civilian bioterrorism, especially with regard to food-born illnesses, there are important differences. A meaningful analysis of biodetection architectures for agrobioterrorism would require a separate study.

2.2 Implications of a Blanket Defense

In order to make these questions more tangible, consider, for example, the type of biodetection architecture that would be needed to protect the citizens of Lincoln, Nebraska, with a population of about 220,000. Based on technologies that currently are available or are likely to become available within the next five years, this would involve deployment of aerosol samplers at a density of about one per square kilometer. These samplers might operate continuously as environmental monitors, and trigger sample collection and analysis following a sensor reading that is above some critical threshold. Alternatively, sample collection might be carried out continuously, although this would place a heavy burden on downstream, high-throughput analytical procedures. In order to cover the city of Lincoln, Nebraska at a spacing interval of two kilometers, approximately 150 sensor stations would be required. The relatively flat topography of Lincoln likely would simplify the deployment of these sensors, allowing something close to regular spacing. A city such as San Francisco would require a more complex deployment strategy in order to ensure complete coverage of its complex topography.

Even on the plains of Lincoln, Nebraska, blanket coverage with a network of biosensors would be very expensive. Each sensor node would cost approximately $100,000, with an annual maintenance cost of approximately $10,000. Perhaps within the next five years the cost of deploying and maintaining each sensor node will decrease by ten-fold. This might not be the case, however, if one considers the cost necessary to keep each node operating at a certified level of performance. Perhaps it is unnecessary to deploy sensors in a blanketed fashion. The population density is much lower in some of the outlying areas of the city, so fewer sensors might be needed there. However, the political ramifications of leaving the rural population "uncovered" could make this strategy unacceptable. Conversely, it likely would be necessary to deploy more sensors in congested areas, such as the city center, and at "high-value" locations, such as the state capitol building, airport terminals, and major shopping malls. And don't forget Memorial Stadium, site of Saturday's nationally televised football game between the Nebraska Cornhuskers and Texas Longhorns!

All of these considerations, and the difficult choices that they present, relate to protection of less than 0.1% of the population of the United States. Whatever is done for the good citizens of Lincoln, Nebraska surely must be done for the residents of Omaha, Sioux City, Davenport, and so on. The nation may decide that it simply must be done. At an amortized cost of roughly $40 per person per year, an effort could be made to provide biodefense coverage for nearly the entire U.S. population. Some might argue that the degree of protection and peace of mind that this would bring would justify the annual expenditure of $10-15 billion. However, there are three complicating factors that must be considered:

1) *The domestic biodefense posture is not one of perimeter defense.* Historically, the problem of defending against biological warfare agents has been addressed on the battlefield, where a perimeter is established that separates allied from enemy forces. The integrity of that perimeter must be guarded against penetration by a biowarfare agent, requiring the deployment of monitoring devices along the perimeter. There is no perimeter with regard to homeland biodefense. The lines of de-

fense can easily be breached because of the open nature of U.S. society and the clandestine manner in which bioterrorism agents can be prepared, transported, and released. Comprehensive biodefense based on biosensors would indeed require a blanket deployment, with the level of expenditure discussed above.

2) *There is a difficult problem of false alarms.* Any technology for continuous environmental monitoring that is even on the horizon will give rise to at least one false alarm per detector per day. This is an optimistic estimate, with a false alarm rate of about ten per detector per day being more realistic. Some areas of deployment will be more susceptible to false alarms, for example, in Lincoln, Nebraska where substantial amounts of pollen grains blow in off the prairie. One could design detector systems that have very low false alarm rates, for example, involving high-throughput sample collection and subsequent quantitative analysis. However, such systems likely would be far too expensive to deploy in a blanketed manner. Every alarm, whether true or false, must be followed up by a secondary analysis. Secondary analysis is performed less frequently but at a higher cost per test compared to primary analysis. A balance must be found between primary and secondary analysis that seeks to minimize the overall cost of the system while ensuring reliable performance. A reasonable estimate for secondary analysis is approximately 25% of the cost of primary analysis, or about $10 per person per year.

3) *A blanket defense against bioterrorism must go far beyond the detection of an airborne release of anthrax.* Again, colored by thinking about battlefield defense, as well as past experience within the U.S. bioweapons program, emphasis has been placed on defending against attacks involving the aerosol distribution of desiccated anthrax spores. Biosensors have been developed that detect other pathogens, but most approaches to continuous environmental monitoring have been directed towards airborne anthrax. There are many possible bioterrorism agents, and

many possible ways in which they can be delivered. Even anthrax spores need not be delivered by an aerosol release, as was made abundantly clear by the events of October, 2001. Delivery though the mail, the produce stand, the theatre turnstile, and the public restroom all are possible, and would be difficult to detect by a network of environmental samplers placed at two-kilometer intervals across the city of Lincoln, Nebraska.

2.3 A Focused, Flexible Deployment Strategy

Notionally, consider a different biodefense posture that involves a focused rather than a blanket sensor deployment. This would entail the flexible deployment of biosensors at high-value locations and in response to specific threats. Memorial Stadium in Lincoln would be considered a high-value location, perhaps not during routine practice sessions, but certainly on the day of a big football game. The airport and state capitol building would be considered high-value locations at all times. Whenever there is an indication of a specific threat based on intelligence data, an extensive sensor deployment would be implemented at the corresponding location. A focused biodefense posture must be nimble, employing an evolving network of sensors to meet evolving threats and vulnerabilities. Compared to a blanket deployment, this posture places greater demands on intelligence information that can help to define the threat. Any information that would reduce the number of sites considered at risk, the types of biological agents that are thought to constitute a realistic threat, and the modes of delivery that are likely to be employed, would guide the deployment of a focused biodefense.

There already is in place a different kind of biodetection network; one that involves 288 million mobile sensors with the capacity to self-report medically significant exposures to a broad range of pathogens. These sensors are prone to noise and, unfortunately, exhibit significant latency between the time of exposure to the pathogen and the generation of a meaningful signal. However, the vast number of such sensors, distributed across the entire country, make them an extraordinarily valuable resource in the aggregate. These mobile biosensors are, of course, the American people. Their value for homeland biodefense should not be stated cavalierly or in a manner that connotes canaries in a coal mine. The reality, however, is that a bioterrorism attack will be felt as a public health emergency, and a pattern of change in the health status of the population is likely to be the first indication that something is amiss.

An effective civilian biodefense calls for a frank assessment of threats and vulnerabilities, and communication of that assessment to the general public so that they can assist in their own defense. The nation's political leaders face an important challenge in bringing these facts to the public. This is a public policy issue, and thus lies outside the scope of a JASON study. It is critical, however, in framing the problem realistically so that resources can be focused appropriately. The effort in public education might begin with a statement such as the following:

> "The government cannot protect everyone against all possible bioterrorist threats. No line of defense that could be established against such threats would be impenetrable. However, the problem is being taken seriously and the government and medical community are working together in preparing to respond. Our top priorities are to protect the basic functions of society and to save as many lives as possible. Resources will be directed toward maintaining medical care services, police and fire protection, electricity, safe drinking water, and the basic forms of government service."

3 PROPOSAL FOR AN INTEGRATED BIODETECTION ARCHITECTURE

3.1 Components of the System

It is important to think in terms of a systems approach to biodetection, rather than individual biosensors. It also is important to realize that the system must involve more than a network of biosensors. A biodetection architecture should be regarded as a system of systems, integrating three key lines of information that feed toward a common analytical point. One of those lines involves the data generated by the network of biosensors. The other two are intelligence gathering and medical surveillance (Figure 1a).

The common analytical point involves a team of local experts who are familiar with local vulnerabilities, high-value targets, and environmental conditions. The team includes members of the public health and medical community, police, fire, and other emergency responders, government officials, and various technical experts (Figure 1b). These individuals meet together on a regular basis to consider potential threats and how best to respond to them. In a major metropolitan area such as Los Angeles the analysis team might consist of 20-30 people, while in a smaller city such as Lincoln, Nebraska it might involve half that number with most participants wearing more than one hat.

The local analysis team is supplied with intelligence information from local, state, and federal resources, and strives to interpret that information with regard to the local context. The team also is responsible for formulating a response posture and directing specific action in the event of a bioterrorism attack. The response should not be formulated on-the-fly, but rather guided by a pre-established "playbook" that prescribes particular responses for a particular set of circumstances. The details of the response will be shaped by

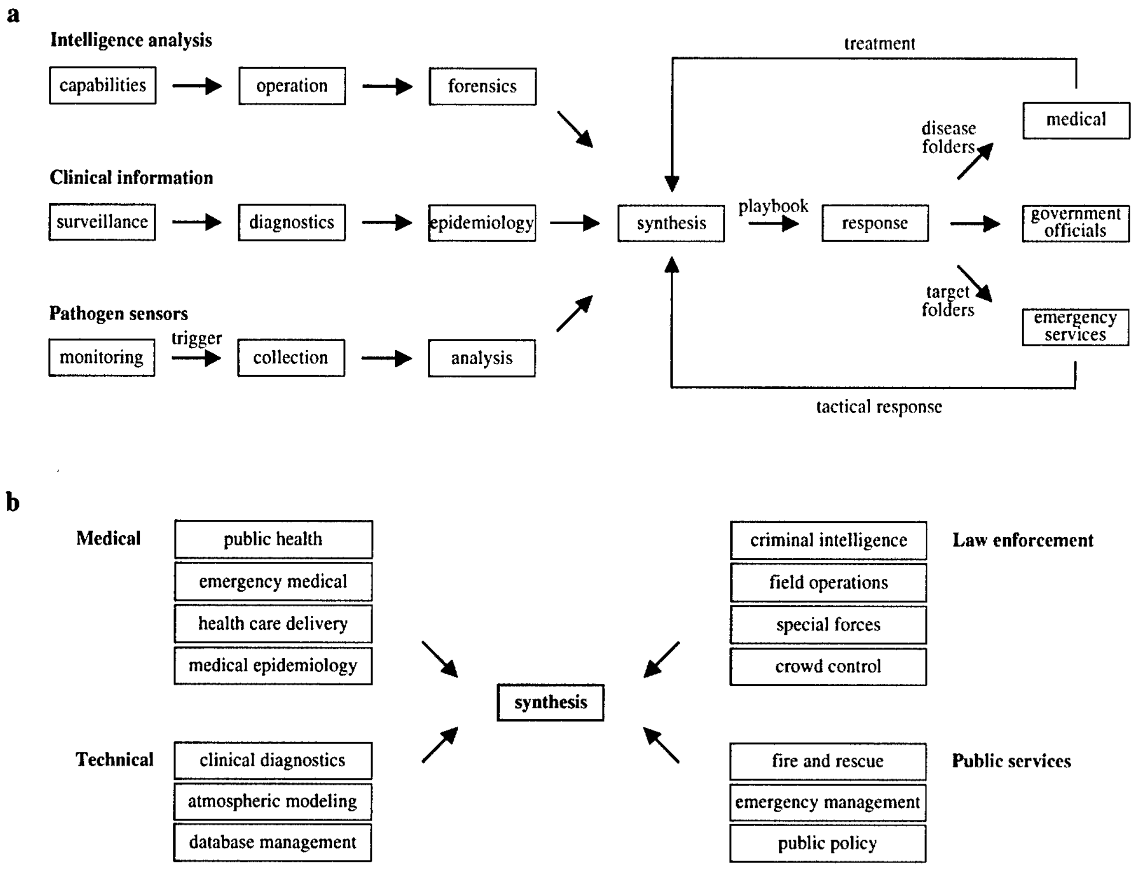


Figure 1: Proposed biodetection architecture. (a) Components of the system, integrating three types of information to direct an effective response. (b) Participants on the local analysis team.

the details of the event, but the playbook provides a framework for mobilizing resources in an effective and integrated manner. The contents of the playbook must be prepared in advance, rehearsed, and revised as necessary.

Response to a bioterrorism incident must be directed by local authorities, assisted by state and federal resources (Figure 1a). Local knowledge is essential in implementing a response that takes into account local geography, medical resources, and emergency response capabilities. The local analysis team has at its disposal a set of "target folders" that provide details regarding each of the high-value locations in the area. The target folder for Memorial Stadium in Lincoln, for example, would include a detailed site plan, with schematics of the stadium and supporting buildings. It would provide information regarding prevailing winds, air handling equipment and other utilities, access routes for emergency vehicles, capabilities of nearby medical facilities, and the location and type of any biosensors that might be deployed.

The local analysis team also has available a set of "disease folders" that provide up-to-date information regarding relevant biological pathogens. For each pathogen, the disease folder describes the characteristics of an associated infection, including presenting symptoms, normal course of disease, degree of communicability (if any), standard and alternative treatments, availability of appropriate medications, and the expected response to treatment. Such information already exists within the medical community, but needs to be continually updated with regard to potential bioterrorism threats and current best practice for the diagnosis and treatment of bioterrorism-related diseases.

The local analysis team remains active as the response plays out, integrating information regarding emergency management and medical treatment with updated information from intelligence sources, medical surveillance systems, and biosensor networks. The team might request additional medical information from particular treatment centers or suggest that additional diagnostic tests be performed. They might direct the deployment of biosensors at specific locations or conduct secondary analyses on previously collected samples. They continue to be guided by the playbook, which describes alternative follow-on responses for different sets of circumstances.

3.2 Intelligence Information

As noted above, any intelligence information that helps to define existing capabilities and intentions for bioterrorism, especially with regard to specific targets, will guide the deployment of a flexible strategy for biodefense and assist in the preparation of an effective response. Information is needed regarding current efforts to develop and deliver bioterrorism agents, as well as forensic analysis of past bioterrorism events. A threat matrix should be developed and updated frequently. This information should be communicated to the local analysis teams, stripped of identifiers regarding sources and methods. In the example of the Salt Lake City Olympics, which will be discussed in detail below, no meaningful intelligence information was provided to the local analysis team. This made it difficult for the team to formulate a response plan because they were required to defend against all possible bioterrorism agents delivered by any means imaginable. Anything that can be done on the intelligence side to reduce or at least prioritize the possibilities will greatly assist the local team in developing a useful response playbook.

JASON is not in a position to formulate a current threat matrix for bioterrorism, which in any case is outside the scope of the present study. As a model, however, for what such a threat matrix might contain, JASON divided the potential threat into five categories, based on the type of organization involved: state sponsored, international terrorist, domestic terrorist, malevolent cult, and crazed individual (Appendix 1a). Each type of organization would be associated with a particular style of attack, set of capabilities, likelihood of attack, and list of biological agents that they might employ.

Corresponding to the threat matrix would be a model response posture, broken down into proactive, defensive, and reactive responses (Appendix 1b). Again, it is beyond the scope of the present study to consider the details of the response posture. In general, this posture would coincide with the various threats, emphasizing that different categories of threat call for different types of responses. For example, state-sponsored bioterrorism might be addressed in a proactive manner by employing diplomacy and deterrence measures, while a proactive response against attack by a crazed individual might involve analysis of criminal databases and closer application of a physicians "duty to warn" based on Tarasoff laws (*Tarasoff v. Regents of University of California*, 17 Cal.3d 425, 1976). The model response posture is formulated at the national level, reflecting intelligence information, technical capabilities, and public policy. The local analysis teams are responsible for interpreting the response posture in terms of the unique characteristics of their particular locale.

3.3 Medical Information

3.3.1 Sources of Information

There are several types of medical information that should be brought to bear, in concert with intelligence information and biosensor information, to assist the local analysis team in recognizing and responding to a bioterrorism attack. First, there is information regarding the biological agents themselves. Much is known about their stability under various environmental conditions, dispersal characteristics, virulence, and communicability. Second, there is information regarding the pathophysiology and clinical course of bioterrorism-associated diseases. This includes the "typical" progression of disease, as well as the range of responses that might occur across a heterogeneous population with varying sensitivities and varying levels of exposure to the biological agent. Third, there is information regarding environmental correlates of disease. Drought conditions, for example, might be conducive to releasing anthrax spores that are latent in the soil, while recent flooding might enhance the mosquito population and promote the spread of certain viral diseases. Fourth, there is information derived from animal sentinels, which might serve as an early indicator of exposure to a pathogen. The distribution of dead crows, for example, has provided an early warning of natural outbreaks of West Nile virus. Disease outbreaks among domestic livestock might provide an early indication of attack with anthrax or certain other pathogens.

A fifth and highly valuable source of medical information pertaining to bioterrorism events is the health status of the U.S. population. The network of 288 million citizen biosensors, if properly harnessed, would provide a critically important component of a biodetection architecture. Patient monitoring can, in principle, be carried out at three different stages relative to the time of exposure to a biological agent (Figure 2). The first is the presymptomatic stage, beginning at the time of exposure and extending to the time of onset of overt symptoms of disease. This is a critical interval, typically lasting one to several days, during which a prompt diagnosis could have a profound effect on reducing the overall morbidity and mortality of a bioterrorism event. For the past several years, JASON and others have been calling for increased research in the area of pre-symptomatic diagnosis. This might involve, for example, analysis of messenger RNA expression levels, measurement of serum levels of cytokines and other circulating proteins, or measurement of small-molecule metabolites that rise or fall with the onset of an infection. Many academic, government, and commercial laboratories have been pursuing these and other approaches to pre-symptomatic diagno-

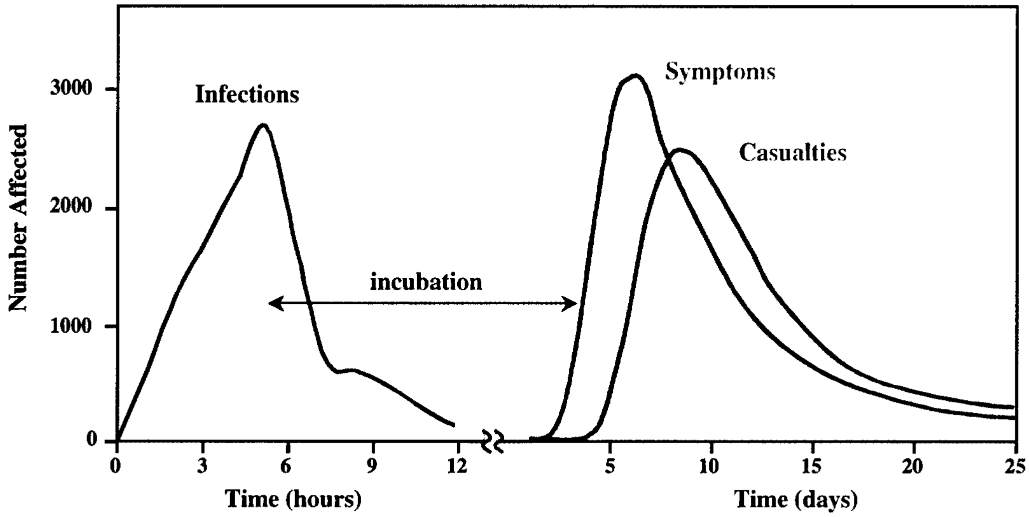


Figure 2: Nominal timeline for a bioterrorism event. There is a substantial lag between the time of infection and the onset of symptoms, and between the onset of symptoms and development of full-blown disease. (Source: *Defense of Cities Study*, The Washington Institute and Sandia National Laboratories).

sis. It must be said, however, that no such method has yet proven effective. This remains an important area for research, but is not likely to be part of a fielded biodetection architecture within the next five years.

The second stage of patient monitoring begins with the onset of the first symptoms of disease and ends with the development of a full-blown infection. This stage can be meaningfully addressed by "syndromic surveillance" of a potentially exposed population. The principle underlying syndromic surveillance is that the earliest symptoms of disease tend to be highly non-specific for a given individual, but often suggestive when considered across an entire population. For example, a sore throat accompanied by upper respiratory congestion would be interpreted for an individual as the onset of a cold or perhaps a seasonal allergy, but if those symptoms occurred almost simultaneously for many individuals within a clustered geographical area, it might suggest something more sinister. If a subset of those individuals then began to experience shortness of breath, suspicion would be raised further, and the possibility of a bioterrorism attack would come to the attention of the local analysis team. In this way the team would be prepared to respond even before the first confirmed case. The sooner a proper response can be organized and implemented, the fewer casualties will result.

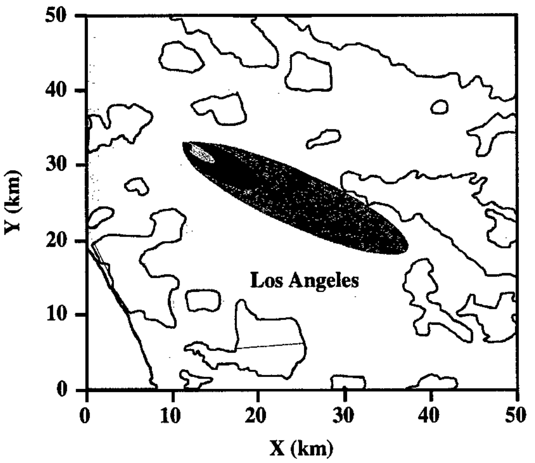
The third phase of patient monitoring pertains to the diagnosis and treatment of disease, again considered across the entire population. Surveillance continues during the response and treatment period, keeping on guard for the possibility of an atypical event. The "disease folders" that are available to the local analysis team describe the range of what is considered typical for each biological pathogen, as well as key indicators that might suggest exposure to a novel or modified agent.

3.3.2 Population Behavior

The local analysis team must integrate the many different types of medical information described above. Their task is facilitated by considering the data in relation to features of the local geographic area. Local knowledge is essential in formulating the best interpretation of the assembled data. Situational awareness at the level of the population has additional benefits resulting from statistical analysis of population behavior. Responses that are averaged across many individuals can point to general trends, while responses from the most sensitive outliers in the population can provide the earliest indication of a bioterrorism attack.

Consider, for example, a point release of airborne anthrax, which then disperses across a densely populated area. Such a release was modeled in the recent *Defense of Cites Study* conducted by The Washington Institute and Sandia National Laboratories (Figure 3). Persons located in the immediate vicinity of the site of release might receive a dose equal to the LD_{50} (the dose fatal to 50% of exposed individuals), although perhaps only a few hundred people would be in a position to receive this level of exposure. As the plume diffuses over a broad area it becomes more dilute, but reaches a much larger number of individuals. Within the outer contours of the plume the level of exposure might be only a small fraction of the LD_{50}, but the number of potentially affected individuals would be so large that even the small fraction of those who developed a fatal infection would be far greater than the number infected close to the site of release. Humans are stochastic responders, potentially capable of becoming infected by even a single pathogenic organism. The lower the dose, the lower the probability of infection, but once an infection takes hold, it becomes amplified due to the replicative properties of the infectious agent.

Mechanical biosensors operate by different principles than human biosensors. A mechanical biosensor must be tuned to some threshold, below which the response is considered "noise" and above which it is considered "signal". Depending on the application, one might choose to lower or raise that threshold, tolerating more "false positives" or "false negatives", respectively. The overall sensitivity of the system might be improved by correlating the behavior of multiple mechanical biosensors. This would fall far short, how-



Contour	Dose / LD_{50}	Population	Infected
■	1	310	170
░	0.1	2,700	750
■	0.01	17,000	1,700
▓	0.001	110,000	2,800
Total	0.001	130,000	5,400

Figure 3: Model release of anthrax spores from a single location in downtown Los Angeles. As the plume spreads it becomes more dilute, but also contacts a much larger number of people. (Source: *Defense of Cities Study*, The Washington Institute and Sandia National Laboratories).

ever, of what could be achieved with a binary filter (infection or no infection) coupled to an exponential amplifier (pathogen replication). The advantages described for human biosensors would apply similarly to animal sentinels and to cell-based devices that incorporate a pathogen-specific amplification mechanism. Such devices are under development, but are unlikely to be deployed within the next five years. The polymerase chain reaction (PCR), while a very powerful signal amplifier, does not have the characteristic of operating in a pathogen-specific manner during successive cycles of amplification. Once a signal is generated during the first cycle of the PCR, it is amplified exponentially, regardless of whether it began as a true or false signal.

3.4 Monitoring Systems

Significant progress has been made in recent years with regard to monitoring the civilian population for early indications of a bioterrorism attack. Many different health monitoring systems have been developed, several of which have been tested in the community. The greatest progress has been made in the area of syndromic surveillance. As discussed above, pre-symptomatic monitoring is not yet practical. Disappointingly little effort has been directed toward the development of systems that monitor the course and treatment of disease, other than for purposes of medical cost management. The various systems that have been developed for syndromic surveillance take into account different types of primary data. Some consider only a handful of key symptoms so that there will be less ambiguity and less effort required at the time of reporting. Other systems strive to be highly inclusive and rely on data mining techniques to abstract useful information. Thus far there has not been a meaningful comparative study of the various systems, which would require side-by-side implementation on a common set of inputs. JASON did not attempt to evaluate the performance of existing syndromic surveillance systems, but strongly urges that comparative testing be done in advance of any large-scale implementation.

One of the systems that considers only a small number of parameters is the Rapid Syndrome Validation Project (RSVP), developed by Sandia National Laboratories and the New Mexico Department of Health. The system tracks six common medical symptoms, together with geographic and temporal information, which are reported via a web-based interface. An alternative medical surveillance system, developed by Los Alamos National Laboratories, is the Biological Surveillance, Analysis, Feedback, Evaluation and Response (B-SAFER) system, which gathers additional information pertaining to clinical signs and some common laboratory tests. One of the systems that adopts a highly information-intensive approach is Real-time Outbreak and Disease Surveillance (RODS), developed at the University of Pittsburgh Medical Center, with funding from DARPA, the Centers for Disease Control, and the National Library of Medicine. (The name "RODS" is a pun, referring to the gram-positive rod *Bacillus anthracis.*) RODS takes into account not only signs and symptoms of disease, but also doctors' hospital orders, results of microbiological tests, and radiological reports. The assembled data then is matched against a set of case definitions that correspond to various bioterrorism-related diseases. When given a demonstration of the RODS system in February, 2002, President Bush remarked: "I had the honor of seeing a demonstration of the modern DEW (Distant Early Warning) line: a real-time outbreak and disease surveillance system."

JASON advocates considering a more active approach to disease surveillance. A limited number of volunteers, either chosen randomly or selected because of their heightened susceptibility to infectious disease, could serve as sentinels for the population at large. These individuals would provide frequently updated information concerning their health status. This could include non-invasive telemetric monitoring of physical signs, for example, measurement of oxygen saturation using a pulse oximeter as an early indicator of respiratory distress. Active surveillance could be enhanced whenever there is an indication of a possible bioterrorism attack. By monitoring the most susceptible individuals most closely, it should be possible to direct treatment to them more quickly, while benefiting the population as a whole by providing the earliest possible warning of an attack.

3.5 Biosensor Information

The third component of a biodetection architecture is the network of deployed biosensors. Information derived from these sensors must be integrated with intelligence and medical information to assist the local analysis team in determining the nature and potential impact of a bioterrorism attack. There are three broad categories of biosensors: continuous environmental monitors, sample collection devices, and rapidly-deployable sensors. All three have a role in a well-structured biodetection architecture. The present study did not evaluate the performance of biosensors that have been deployed or currently are under development. For more information on this topic see the 2001 JASON Report on "Biosensing" (JSR-01-100). Examples of biosensors from each of the three broad categories will be discussed below in order to illustrate how each could fit into a biodetection architecture.

3.5.1 Environmental Monitors

Continuous environmental monitors operate in the field in an automated or semi-automated fashion. They usually are placed at fixed locations, although proposals for mobile continuous environmental monitors have been considered. All of the devices that have been fielded thus far draw in air samples that are filtered and concentrated for analysis. A similar approach might be taken for water sampling or contact sampling of solid objects. One example of a continuous air sampler is the Biological Aerosol Warning System (BAWS), developed by Lincoln Laboratories (Appendix 2a). It analyzes particles of 2-10 microns in diameter by exciting them with short-wavelength ultraviolet light, then measuring the UV-visible fluorescence emission spectrum. This provides a "fingerprint" corresponding to various biological compounds, such as tryptophan-containing proteins, purine derivatives, and flavins. Pattern analysis algorithms are used to distinguish between, say, *Bacillus* spores and pollen grains. The detection limit of the BAWS device is ~25 agent-containing particles per liter of air, with an associated rate of false-positives of 10-100 per day, depending on location.

Continuous environmental monitors do not allow definitive identification of bioterrorism agents. They function largely as change detectors that are especially sensitive to particles that have some pre-determined set of characteristics. They can be used to trigger more definitive analysis, which would require some form of sample collection. The chief advantage of continuous environmental monitors is their relatively low cost, especially the low cost of consumables, compared to sample collection and analysis. The chief disadvantage is that they cannot be optimized to detect a broad range of pathogens in the face of a complex and changing environment.

3.5.2 Sample Collection Devices

The second broad category of biosensors entails sample collection devices. These devices either collect samples which then are returned to a central laboratory for analysis, or perform both collection and analysis in the field and report the results electronically. An example of a system for sample collection and subsequent laboratory analysis is the Biological Aerosol Sentry and Information System (BASIS), developed by Lawrence Livermore and Los Alamos National Laboratories (Appendix 2b). The device collects aerosol samples over a 1-24-hour period, gathering material on filter papers which then are transported to the laboratory for sample processing and analysis by quantitative PCR (Q-PCR). The development of reliable Q-PCR assays for the detection of a host of bioterrorism agents should be considered part of "the system". As currently fielded, BASIS tests for four bioterrorism-related pathogens: *Bacillus anthracis (anthrax)*, *Brucella sp.* (brucellosis), *Francisella tularemia* (tularemia), and *Yersinia pestis* (plague). Additional tests are being developed, with a typical development time of only a few months per test. The tests are highly sensitive, with a current threshold for detection of >800 organisms, which might be reduced to >100 organisms within the next few years. The frequency of false positives is ~1% per individual test, although most of these can be excluded by performing a secondary test that examines other genetic loci within the same organism. In practice, the primary and secondary tests are carried out concurrently or in close succession so that a response is not based on the results of a single test.

The chief limitation of sample collection devices such as BASIS is their cost of operation. While Q-PCR analysis itself is automated, transporting samples to the laboratory and preparing them for Q-PCR analysis are both labor intensive. There also are substantial reagent costs, typically about $1 per test, and some of the reagents must be maintained under controlled storage conditions. Lawrence Livermore National Laboratories is completing the development of a second-generation device that carries out both collection and analysis in the field. This is the Autonomous Pathogen Detection System (APDS), which can operate unattended for 24 hours and can test for multiplepathogens employing either Q-PCR or antibody-based technology (Appendix 2c). Systems such as APDS present a trade-off between reduced labor costs and increased cost of operation per unit compared to systems that involve sample collection followed by analysis at a central facility. Because of the extreme sensitivity of the diagnostic tests, considerable effort is required to maintain quality-control standards for sample handling and instrumentation. It would be far more challenging to maintain those standards for a distributed set of autonomous devices compared to the controlled environment of a common diagnostic laboratory.

3.5.3 Rapidly-Deployable Sensors

The third broad category of biosensors entails rapidly-deployable sensors, ranging from drop-on-target detectors to hand-held analytical devices. While many sensors of this type have been developed, few of them provide sufficiently reliable information across a broad range of pathogens to be a useful component of a biodetection architecture. One notable exception is the Handheld Advanced Nucleic Acid Analyzer (HANAA), developed at Lawrence Livermore National Laboratories, which performs four-channel Q-PCR (Appendix 2d). This device weighs only five pounds (including batteries) and provides definitive results within four hours from the time of sample collection. It still requires manual sample preparation and must be preconfigured for a particular set of tests before being taken into the field. However, easy portability make this and similar devices an important component of a flexible biodefense that relies on an evolving network of sensors to address evolving threats and vulnerabilities.

3.5.4 Integrated Sensor Deployment

The biosensor portion of a biodetection architecture likely would include devices from each of the three broad categories discussed above. Continuous environmental monitors might be placed at choke points such as airport access roads, water treatment plants, and food distribution centers. Sample collection devices might be placed at high-risk locations such as government buildings, major sports facilities, and national landmarks. Rapidly-deployable sensors might be distributed on short notice to the site of a specific threat or suspicious incident. All of these sensors must be related to geographic and temporal information and coordinated in their operation. Data collected from the various biosensors should be fused with other types of sensor information, such as video surveillance, traffic analysis, and meteorological data. The goal is to provide the local analysis team with situational awareness so that they can recognize patterns of unusual occurrence at the earliest opportunity.

4 BIODEFENSE AT THE 2002 SALT LAKE CITY OLYMPICS

It is highly instructive to consider an example of the real-world deployment of a biodetection architecture, as took place at the 2002 Winter Olympic Games in Salt Lake City. In light of the catastrophic events of September 11 and the subsequent anthrax incidents of October, 2001, there was genuine concern that a bioterrorism attack might occur at the Olympic Games. The Olympic Organizing Committee and the nation had an obligation to protect the athletes, workers, spectators, and local citizens against bioterrorism. This obligation was taken very seriously and pursued with considerable resources.

Two of the three components of a sound biodetection architecture were deployed at the Salt Lake City Olympics, drawing on both medical and biosensor information, but without significant input of intelligence information. Two local analysis teams were formed, one focusing on technical issues and the other on policy issues. Both teams served a purely advisory function and were not given the authority to direct a response. Medical information was delivered through implementation of RODS syndromic surveillance at primary care centers throughout the region, covering ~75% of all acute care visits. Four continuous environmental monitors and 16 sample collection devices were deployed at critical locations, including the airport, city center, and some of the athletic venues. The continuous environmental monitors were Joint Biological Point Detection System (JBPDS) aerosol samplers, similar to the BAWS device. The sample collection instruments were BASIS units, collecting material over successive four-hour intervals. The samples were transported to a central laboratory for analysis. In addition, there was random testing of the mail at three different postal facilities. This was by no means a blanket deployment, which would have been far too expensive to implement. Furthermore, the BASIS analysis was limited to the detection of anthrax, brucellosis, tularemia, and plague.

The technical and policy advisory groups were established well in advance, and had the opportunity to develop and refine their "playbook" with regard to potential bioterrorism events. Without the benefit of any intelligence information, however, they had no idea what to expect, other than the vague possibility of inhalation anthrax or something worse. The FBI had a significant presence at the Salt Lake City Olympics, but their focus, as has traditionally been the case, was on tracking suspicious individuals rather than providing advice for biodefense.

During the two weeks of the Olympics, the RODS deployment tracked ~3,000 primary care visits and did not reveal any statistical anomalies. There were the usual minor outbreaks of infectious diseases at the Olympic Village and two small-scale food poisoning incidents that did not appear to be suspicious. The samples from each of the BASIS units (~100 total samples per day) were subjected to a first-phase screen involving Q-PCR analysis of a single genetic locus for each of the four target organisms. The first-phase screen produced about one false-positive per day, triggering a second-phase screen that involved a repeat Q-PCR analysis, in triplicate, of that same genetic locus. If the second-phase screen also proved positive, then there would be heightened concern and a third-phase presumptive test would be carried out involving Q-PCR analysis of the original plus five additional genetic loci from the same organism. A positive result for the presumptive test would initiate an interagency conference call and likely trigger an emergency response. A confirmatory test would be carried out involving DNA sequence analysis of the PCR product, and additional samples might be collected to better define the nature of the incident.

The morning of Tuesday, February 12 (day 5 of the Olympics) began with an announcement from Attorney General Ashcroft that a heightened state of alert was in effect based on an FBI warning of an increased risk of terrorist activity. At 5:30 pm that day the BASIS laboratory reported a second-phase positive screen for anthrax on a single BASIS unit in a terminal area at Salt Lake City Airport for the 10:00 am - 2:00 pm collection period.

No other units gave even a first-phase positive result for that same collection period. The technical and policy advisory groups convened at the laboratory as the third-phase presumptive test was underway. Utah Governor Leavitt was notified and arrived at the laboratory at about 7:00 pm. He was briefed on the situation and received a quick tutorial on the nuances of Q-PCR. He decided to place the airport "on alert", but recommended that it be kept open pending the results of the third-phase presumptive test.

At 7:30 pm the results of the third-phase test were reported to be negative. At 9:00 pm the results of the first-phase screen for the same BASIS unit for the 2:00 pm - 6:00 pm period also were reported to be negative. Everyone breathed a sigh of relief. A press conference was called at 10:00 pm to report the "non-incident", and within 24 hours the story disappeared from the news wires.

The deployment at the Salt Lake City Olympics, and especially the events of February 12, were a useful exercise in bioterrorism defense. Everyone that was involved took their role seriously because they viewed it as "the real thing". Many lessons were learned regarding both technical and organizational issues. Surprisingly, however, no formal study has been undertaken to assess what proved most effective and what might have been done differently. Anecdotally, one of the key lessons was the need to move as soon as possible from tabletop planning to the actual deployment of a biodetection architecture. A flexible biodefense strategy should allow for ongoing modification of the system, but it is difficult to know what modifications are needed until there is some form of deployment. In Salt Lake City, for example, it would have been beneficial to have the system for syndromic surveillance in place long before the Olympics began so that baselines could be established. The technical advisory group should have had the opportunity to practice with real data before the world's attention was focused on Salt Lake City.

5 THE BIOLOGICAL DEFENSE INITIATIVE

During the second half of 2002, a large-scale test deployment of a biodetection architecture is taking place in Albuquerque, New Mexico. This is the Biological Defense Initiative (BDI), which is being conducted by the DoD Defense Threat Reduction Agency (DTRA), with technical assistance from the DOE National Nuclear Security Administration (NNSA). It involves deployment of medical syndromic surveillance systems, including both RSVP and B-SAFER, as well as an assortment of environmental monitors and biosensors. The stated goals of the BDI are two-fold: first, early detection of bioterrorism events in an urban area and at high-value locations, seeking to minimize casualties; second, integration of environmental modeling, choke point monitoring, medical information systems, and laboratory analysis. The deployment is occurring during June-November, 2002, culminating in a technology "demonstration" in December, 2002.

While the stated goals of the BDI are admirable, the present implementation does not focus on providing a true test of the system. Unlike the Salt Lake City Olympics, the BDI is not motivated by the perceived threat of a bioterrorism attack. The demonstration event in December is likely to be more of a biosensor "festival" than a rigorous comparison of alternative biosensor technologies. Medical surveillance systems are being implemented, but the data that they generate are not being integrated with intelligence and biosensor information. Four different types of biosensors are being fielded, with a total of 35 instruments generating ~1,000 samples per day. The best that can be hoped for from all of these data is that there will be some interesting false positives. These are unlikely to rise to the level that New Mexico Governor Johnson would need to decide whether to close the Albuquerque airport. In the absence of a perceived threat, a useful exercise the system should at least involve a pre-defined set of questions that are to be addressed. Unfortunately, this does not appear to be the case in Albuquerque.

On the positive side, the BDI does involve a real-world deployment of components of a biodetection architecture. Some *ad hoc* lessons are bound to emerge, which would not be the case if this were merely a tabletop exercise. Perhaps the experience will suggest how to conduct more meaningful exercises in the future. Such exercises would involve an extended period of deployment in order to measure local baselines. They also would involve predefined tests of the system through a series of staged events. These events would be designed to assess sensitivity levels, noise rejection, and the ability to reconcile conflicting information. They would test the operation of the local analysis team and local responders as well as the data-generating portion of the biodetection architecture.

A staged bioterrorism event would seek to exercise all components of the system and test how these components interact. It might involve mock intelligence reports, mock sensor data (or sensor data triggered by simulants), and mock medical information involving actors who present themselves at local primary care facilities with staged symptoms. Some false or misleading information might be included to provide greater realism. The local analysis team would be required to play out a series of responses, and the consequences of those response also would be staged. Such a *bona fide* exercise of the system will require careful planning, similar to the planning that occurs for a military exercise. It will be important to vet the planned exercise with an outside panel of experts to ensure that it will be realistic and informative. The same panel also might be asked to conduct a formal analysis of the exercise following its completion. Substantial cooperation will be required from the local community, similar to what has been provided by the town of Framingham, Massachusetts in a comprehensive study of cardiovascular disease. A "Request for Invitation" (RFI) could be issued, seeking a small- to medium-sized city that would be willing to serve as a test bed for the deployment and refinement of a biodetection architecture.

It has often been stated, by JASON and others, that defense against bioterrorism will have substantial dual benefit for public health. Money that is spent on syndromic surveillance, for example, could reduce morbidity and mortality related to influenza and other infectious diseases. This presumed benefit has never been quantified, although many believe it could outweigh the cost of deployment of a biodetection architecture. A test deployment would provide an opportunity to measure the dual benefit directly. This data would help to shape public debate on biodefense and encourage civic leaders to respond favorably the next time an RFI for biodetection is issued. It would point out those features of a biodetection architecture that are most cost effective in view of cost offsets related to improved public health.

This Page Intentionaly
Left Blank

6 ADDITIONAL RECOMMENDATIONS

6.1 Biodefense Working Group (BWG)

It would be beneficial to assemble a group of technical and policy experts who could assist in the planning and analysis of biodetection exercises. This group could begin by evaluating the experience at the Salt Lake City Olympics and other recent deployments. They could analyze the results of the BDI, and consider how such exercises might be made more informative in the future. The BWG could examine the public health implications of biodefense activities, and recommend how greater synergism could be achieved between biodefense and public health. Finally, the BWG could summarize their findings for distribution to local analysis teams throughout the country, which would assist them in developing playbooks to respond effectively to bioterrorism attacks.

6.2 Biological Emergency Search Team (BEST)

While major metropolitan areas have substantial resources that can be brought to bear in the event of a bioterrorism incident, smaller locales might need external assistance, especially during the acute stage of an emergency. Analogous to the DOE Nuclear Emergency Search Team (NEST), it would be beneficial to establish a team of experts who could mobilize rapidly in the event of a bioterrorism attack, bringing special equipment and expertise to the scene. The team might include members from DOE, DoD, DHS, HHS, FBI, and FEMA, with expertise in microbiology, medical diagnostics, epidemiology, climate modeling, criminal intelligence, and emergency response. They could be deployed within 24 hours to any location in the country, where their objective would be to search for, identify, and contain any biological attack. They would work closely with the local analysis team to augment local capabilities. BEST also could serve as a “red team” for planning biodefense exercises. This will sharpen the skills of BEST and challenge those conducting the exercises to address previously unrecognized vulnerabilities.

6.3 Public Education

There is an obligation to educate the public regarding biodefense because a prudent response by the public is critical to minimizing the consequences of a bioterrorism attack. Through ongoing public education, at both the local and national levels, the public must be taught how to recognize and respond to an attack. The focus should be on containment, emphasizing timely reporting of medical symptoms, the practice of good hygiene, and strict adherence to prescribed medical treatments. Conscientious hand washing alone could significantly reduce the morbidity and mortality of a bioterrorism incident (and of infectious diseases in general). Frequently Asked Questions (FAQ) sheets should be made available pertaining to the various bioterrorism-related diseases. The public should be able to access this information readily, by telephone and on the web. Finally, as was clear from the anthrax incidents of October, 2001, it is important to designate a credible national biodefense spokesperson who can present timely and accurate information to the public. That person must be both technically informed and aware of the relevant public policy issues. He or she should be able to state the facts as they are known and reinforce the lessons of a prudent civilian response as taught by the prior public education efforts.

7 CONCLUSIONS

JASON does not see justification for a blanket deployment of biosensors for homeland biodefense. It envisions focused deployment at high-value locations and in response to specific threats. The public needs to be made aware of the reasons for this posture and told that they provide the most important component of an effective biodetection architecture. That architecture is a system of systems, drawing upon intelligence information, medical information, and biosensor data. The gathering point for that information is the local analysis team, armed with target folders pertaining to local facilities and disease folders pertaining to the various bioterrorism agents. The local analysis team will have developed a playbook to guide their response to different circumstances, and will have practiced those responses. Should a bioterrorism attack occur, the local authorities will be assisted by an informed public in their efforts to maintain order and minimize casualties.

This Page Intentionaly
Left Blank

A APPENDIX

a

Organization	**Style of attack**	**Capability**	**Likelihood**	**Agents**
State-sponsored (e.g. Iraq)	Covert operations against military and strategic targets	Sophisticated	Low	Anthrax, plague, ricin, botulinum toxin, foot & mouth, smallpox?
International terrorist (e.g. Al Qaeda)	Sensational acts against targets of political toxin significance	Modest	Modest	Anthrax, ricin, botulinum toxin
Domestic terrorist (e.g. T. McVeigh)	Vengeful acts against symbols of authority	Rudimentary	Modest	Anthrax, ricin, botulinum toxin
Malevolent cult (e.g. Aum Shinrikyo)	Eclectic behaviors against society	Rudimentary	Low	Anthrax, *Salmonella*
Crazed individual (e.g. Unabomber)	Hostile expressions of personal grievances	Rudimentary	Low	Anthrax, *Salmonella*

b

Organization	**Proactive**	**Defensive**	**Reactive**
State-sponsored	• Foreign intelligence • Diplomacy • Deterrence • Preemptive action	• Protect health system, public services, and continuity of government • Defend population centers	• Diplomacy • Retaliation
International terrorist	• Foreign intelligence • Blocking of resources • Preemptive action	• Protect high-value and high-visibility targets • Defend population centers	• Retribution
Domestic terrorist	• Share information among local, state, and federal law enforcement • Control sensitive materials	• Protect government facilities and critical infrastructure • Threat-specific protection	• FBI investigation supported by state and local law enforcement
Malevolent cult	• Assessment of capabilities • Informants • Infiltration	• Threat-specific protection	• FBI investigation supported by state and local law enforcement
Crazed individual	• Linked criminal databases • Duty to warn based on Tarasoff laws	• Threat-specific protection	• FBI investigation supported by state and local law enforcement

Figure A-1: Intelligence information pertaining to bioterrorism. (a) Model threat matrix. (b Corresponding model response posture.

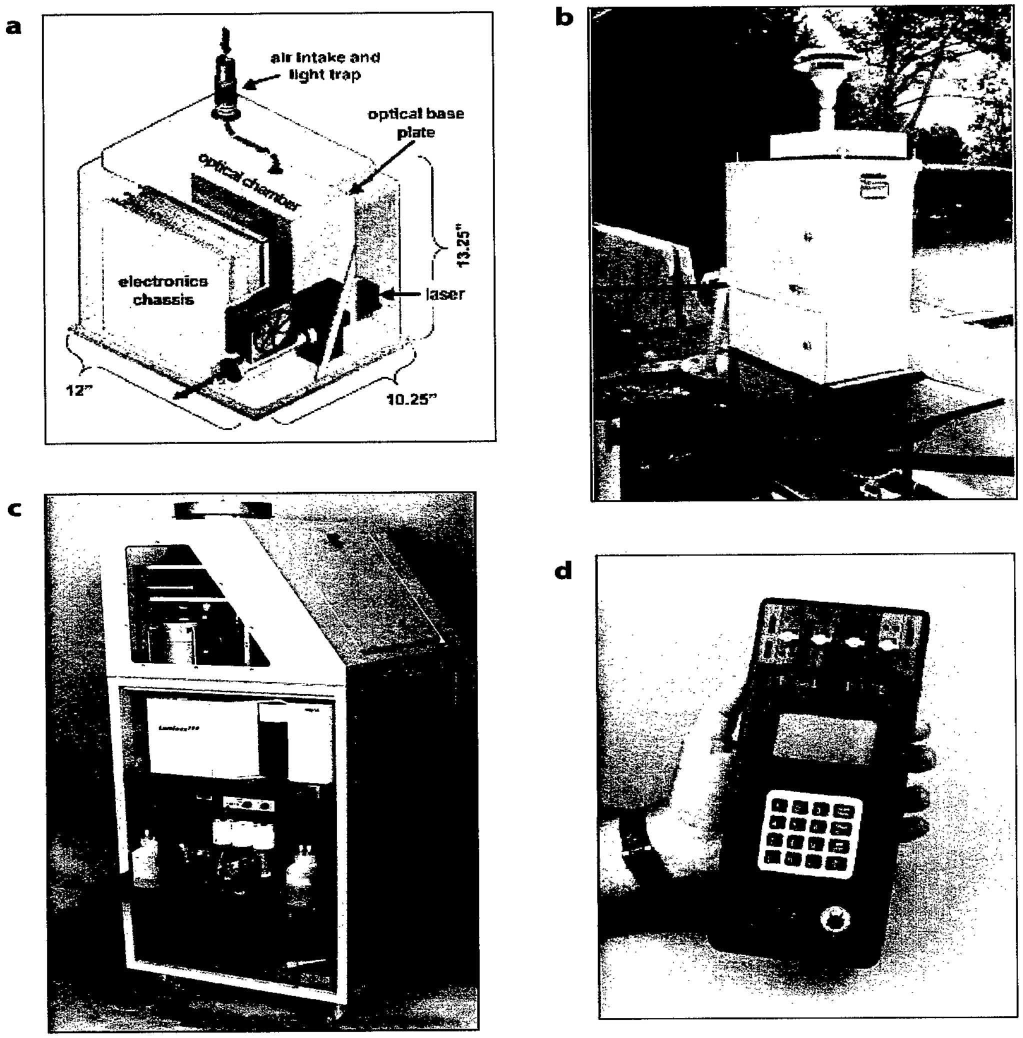


Figure A-2: Biosensor devices. (a) Biological Aerosol Warning System (BAWS), developed by Lincoln Laboratories; (b) Biological Aerosol Sentry and Information System (BASIS), developed by Lawrence Livermore and Los Alamos National Laboratories; (c) Autonomous Pathogen Detection System (APDS), developed at Lawrence Livermore; (d) Handheld Advanced Nucleic Acid Analyzer (HANAA), developed at Lawrence Livermore.

DISTRIBUTION LIST

Director of Space and SDI Programs
SAF/AQSC
1060 Air Force Pentagon
Washington DC 20330-1060

CMDR & Program Executive Officer
U S Army/CSSD-ZA
Strategic Defense Command
PO Box 15280
Arlington, VA 22215-0150

DARPA Library
3701 North Fairfax Drive
Arlington, VA 22203-1714

Assistant Secretary of the Navy
(Research, Development & Acquisition)
1000 Navy Pentagon
Washington, DC 20350-1000

Principal Deputy for Military Application [10]
Defense Programs, DP-12
National Nuclear Security Administration
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

Superintendent
Code 1424
Attn: Documents Librarian
Naval Postgraduate School
Monterey, CA 93943

DTIC [2]
8725 John Jay Kingman Road
Suite 0944
Fort Belvoir, VA 22060-6218

Strategic Systems Program
Nebraska Avenue Complex
287 Somers Court
Suite 10041
Washington, DC 20393-5446

Headquarters Air Force XON
4A870 1480 Air Force Pentagon
Washington, DC 20330-1480

Defense Threat Reduction Agency
Attn: Dr. Arthur T. Hopkins [12]
6801 Telegraph Road
Alexandria, VA 22310

IC JASON Program [2]
Chief Technical Officer, IC/ITIC
2P0104 NHB
Central Intelligence Agency
Washington, DC 20505-0001

JASON Library [5]
The MITRE Corporation
WA549
7515 Colshire Drive
McLean, VA 22102

U. S. Department of Energy
Chicago Operations Office Acquisition and
Assistance Group
9800 South Cass Avenue
Argonne, IL 60439

Dr. Allen Adler
Director
DARPA/TTO
3701 N. Fairfax Drive
Arlington, VA 22203-1714

Dr. Jane Alexander
Office of Naval Research
800 North Quincy Street
Arlington, VA 22217-5000

Dr. A. Michael Andrews
Director of Technology
SARD-TT
Room 3E480
Research Development Acquisition
103 Army Pentagon
Washington, DC 20310-0103

Dr. William O. Berry
Director
Basic Research ODUSD(ST/BR)
4015 Wilson Blvd
Suite 209
Arlington, VA 22203

Dr. Albert Brandenstein
Chief Scientist
Office of Nat'l Drug Control Policy Executive
Office of the President
Washington, DC 20500

Ambassador Linton F. Brooks
Under Secretary for Nuclear Security/
Administrator for Nuclear Security
1000 Independence Avenue, SW
NA-1, Room 7A-049
Washington, DC 20585

Dr. Steve Buchsbaum
DARPA/STO
3701 N. Fairfax Drive
Arlington, VA 22203-1714

Dr. Darrell W. Collier
Chief Scientist
U. S. Army Space & Missile Defense Command
PO Box 15280
Arlington, VA 22215-0280

Dr. James F. Decker
Principal Deputy Director
Office of the Director, SC-1
Room 7B-084
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

Dr. Patricia M. Dehmer [5]
Associate Director of Science for Basic Energy
Sciences, SC-10
Office of Science
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20874

Ms. Shirley Derflinger [15]
Technical Program Specialist
Office of Biological & Environmental
Research, SC-70
Office of Science
U.S. Department of Energy
19901Germantown Road
Germantown, MD 20874

Dr. Martin C. Faga
President and Chief Exec Officer
The MITRE Corporation
N640
7515 Colshire Drive
McLean, VA 22102

Mr. Dan Flynn [5]
Program Manager
DI/OTI/SAG
5S49 OHB
Washington, DC 20505

Ms. Nancy Forbes
Senior Analyst
DI/OTI/SAG 5S49 OHB
Washington, DC 20505

Dr. Paris Genalis
Deputy Director
OUSD(A&T)/S&TS/NW
The Pentagon, Room 3D1048
Washington, DC 20301

Mr. Bradley E. Gernand
Institute for Defense Analyses
Technical Information Services
Room 8701
4850 Mark Center Drive
Alexandria, VA 22311-1882

Dr. Lawrence K. Gershwin
NIC/NIO/S&T
2E42, OHB
Washington, DC 20505

Brigadier General Ronald Haeckel
U.S. Dept of Energy
National Nuclear Security Administration
1000 Independence Avenue, SW
NA-10 FORS Bldg
Washington, DC 20585

Dr. Theodore Hardebeck
STRATCOM/J5B
Offutt AFB, NE 68113

Dr. Robert G. Henderson
Director
JASON Program Office
The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

Mr. O' Dean P. Judd
Los Alamos National Laboratory
Mailstop F650
Los Alamos, NM 87545

Dr. Bobby R. Junker
Office of Naval Research
Code 31
800 North Quincy Street
Arlington, VA 22217-5660

Dr. Andrew F. Kirby
DO/IOC/FO
6Q32 NHB
Central Intelligence Agency
Washington, DC 20505-0001

Dr. Anne Matsuura
Army Research Office
4015 Wilson Blvd
Tower 3, Suite 216
Arlington, VA 22203-21939

Dr. Maureen I. McCarthy
Homeland Security
Anacostia Naval Annex
Building 410
250 Murray Lane, SW
Washington, DC 20509

Dr. Thomas Meyer
DARPA/ATO
3701 N. Fairfax Drive
Arlington, VA 22203

Dr. Julian C. Nall
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

Dr. C. Edward Oliver [5]
Associate Director of Science for Advanced
Scientific Computing Research, SC-30
U.S. Department of Energy
19901Germantown Road
Germantown, MD 20874

Mr. Raymond L. Orbach
Director, Office of Science
U.S. Department of Energy
1000 Independence Avenue, SW
Route Symbol: SC-1
Washington, DC 20585

Dr. Ari Patrinos [5]
Associate Director
Biological and Environmental Research
SC-70
US Department of Energy
19901 Germantown Road
Germantown, MD 20874-1290

Dr. John R. Phillips
Chief Scientist, DST/CS
2P0104 NHB
Central Intelligence Agency
Washington, DC 20505-0001

Records Resource
The MITRE Corporation
Mail Stop W115
7515 Colshire Drive
McLean, VA 22102

Dr. Ronald M. Sega
DDR&E
3030 Defense Pentagon,
Room 3E101
Washington, DC 20301-3030

Dr. Dan Schuresko
Acting Director
National Security Space Architect
PO Box 222310
Chantilly, VA 20153-2310

Dr. John Schuster
Submarine Warfare Division
Submarine, Security & Tech
Head (N775)
2000 Navy Pentagon, Room 4D534
Washington, DC 20350-2000

Dr. Richard Spinrad
US Naval Observatory
Naval Oceanographers Office
3450 Massachusetts Ave, NW
Building 1
Washington, DC 20392-5421

Mr. John P. Sullivan
Emergency Operations Bureau
1275 N. Eastern Avenue
Los Angeles, CA 90063-3217

Mr. Anthony J. Tether
DIRO/DARPA
3701 N. Fairfax Drive
Arlington, VA 22203-1714

Dr. George W. Ullrich [3]
OSD [ODUSD(S&T)]/WS
Director for Weapons Systems
3080 Defense Pentagon
Washington, DC 20301-3080

Dr. Bruce J. West
FAPS
Senior Research Scientist
Army Research Office
P. O. Box 12211
Research Triangle Park, NC 27709-2211

Dr. Linda Zall
Central Intelligence Agency
DS&T/OTS
3Q14, NHB
Washington, DC 20505-00