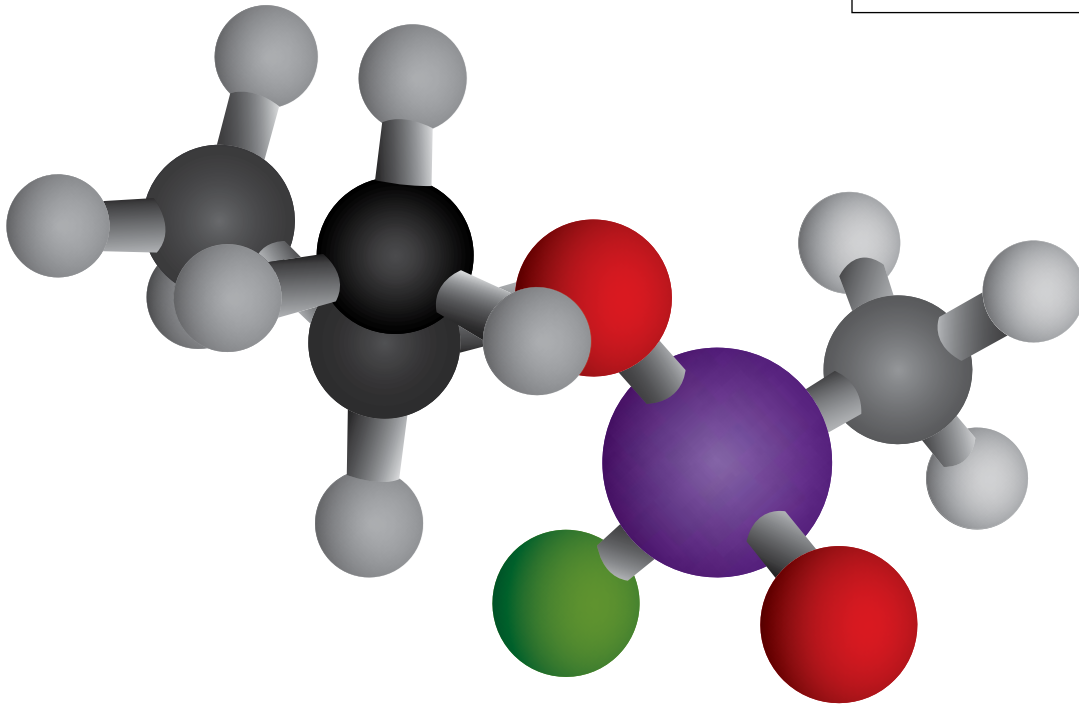
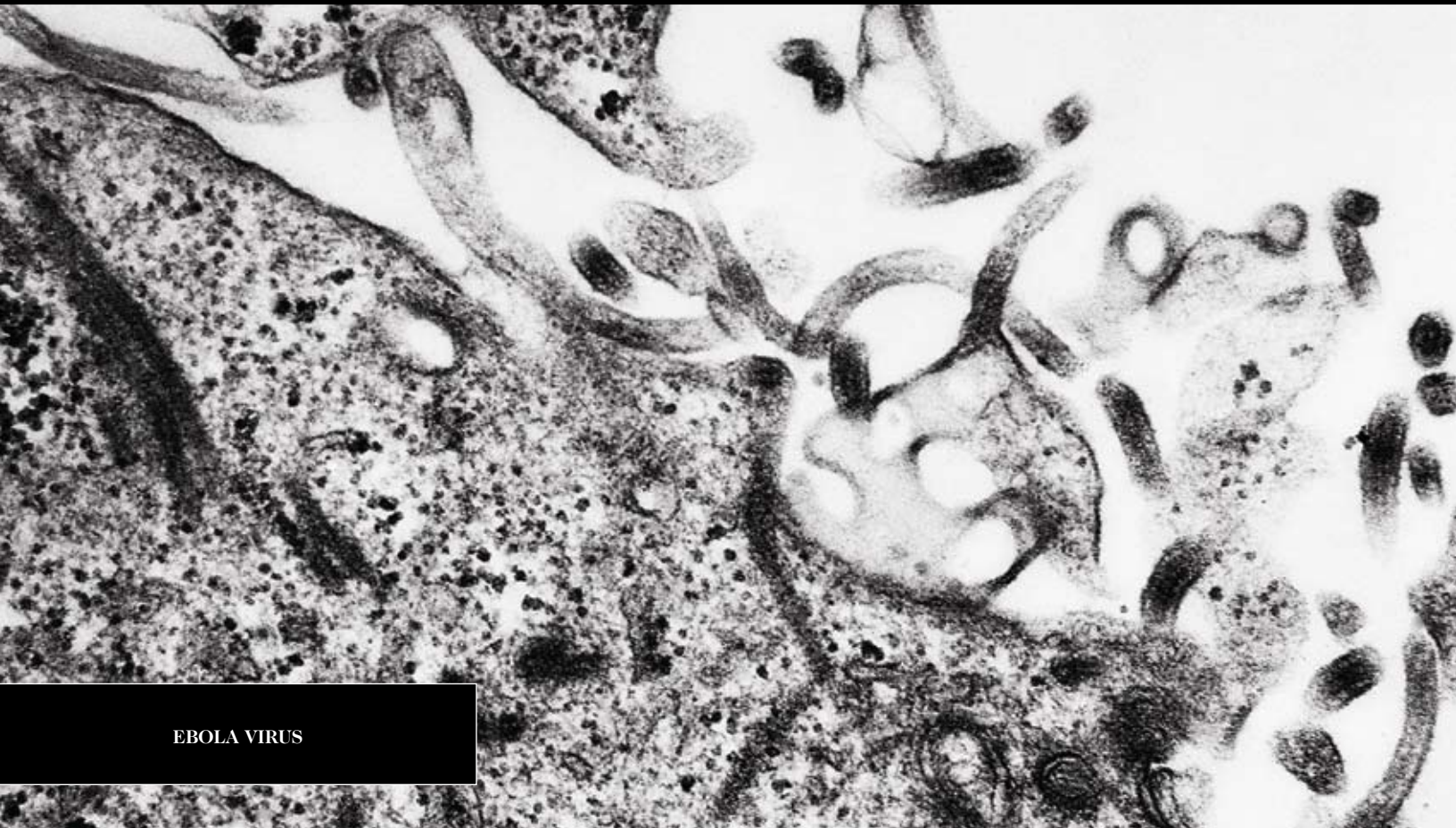


SARIN GAS MOLECULE



CHEMICAL & BIOLOGICAL THREATS: SURVEILLANCE AS THE FIRST LINE OF DEFENSE



EBOLA VIRUS



EXECUTIVE SUMMARY

“Without an environmental warning, the first notification that we have been attacked will be when those tens of thousands of people start getting sick and go to the emergency departments and their doctors’ offices. By then, the game is up. It’s too late. We will have lost that war.”

- Dr. Jeffrey Runge, Assistant Secretary for Health Affairs, Department of Homeland Security, Testimony before the Subcommittee on Homeland Security, House Committee on Appropriations, April 3, 2008.

Chemical and biological agents, whether in the form of weapons employed by terrorists or rogue states, toxic spills or naturally occurring pandemics, pose a significant risk to the U.S. homeland. The threat is growing due to the enhanced globalization and mobility of society, the explosion in chemical and biotech expertise and the resulting ease with which chemical weapons can be created and pathogens can be covertly grown, prepared, transported and released.

Early and accurate detection, characterization and warning of a chemical or biological event are critical to an effective response. To achieve these objectives, an integrated system of sensors is needed. This is particularly the case for a biological event. In the case of a biological outbreak in a heavily populated or traveled area, large numbers of people could be infected. However, biological agents have a latency period during which the infected individuals can transmit the disease but also during which antibiotics can prevent its outbreak. Every hour of early warning is critical and specific techniques for detecting and initiating an early response against these threats are required in advance of the onset of symptoms among the infected population. The impact an early warning system can make is literally the difference between life and death.

Although work remains to be done to improve the effectiveness of chemical threat sensors, the greatest need is for better biological sensors and a supporting information technology network. The current generation of biological sensors is deployed on a limited basis in some 30 large urban environments. They collect airborne particles onto solid filters that are collected manually every 24 hours and transported for analysis to state and local public health laboratories. This is a relatively slow, labor-intensive, expensive and inadequate approach to a nationwide surveillance system.

The next generation of biological sensors will need to be more sensitive and capable of autonomous screening to include both pathogen detection and identification of multiple threat agents such as bacteria, spores, viruses and toxins. The ideal system also would be much less labor intensive, requiring substantially less direct involvement for routine operations. Additionally, it would be able to communicate securely and wirelessly in real- or near-real-time. An improved system exists and could be widely deployed within a few years if adequate funding were made available.

J. Michael Barrett and Daniel Goure, Ph.D.



INTRODUCTION

It has been nearly eight years since the September 11, 2001 terrorist attacks against the United States. Though the collective perceptions of the threat and likelihood of future terrorist attacks have evolved over time, the simple fact is that the United States does not and cannot know if or when it will be attacked again. What is known, having suffered mightily on that terrible day and given the enormity of the potential death and devastation from chemical, biological and other weapons, is that the nation must take every reasonable step to adequately defend itself from the worst of the threats it faces. The health and economic consequences from massive food contamination and Hurricane Katrina reshaped the scope of all-hazards threats, and highlighted the urgency of a more robust biodefense approach. The United States must also be better prepared to minimize the prolonged economic devastation and loss of confidence in government that could accompany an event causing lengthy quarantines and affecting agriculture or the nation's food supply – whether naturally occurring or man-made.

The reality of simultaneously managing these multiple, significant threat vectors is, however, at odds with another reality: the nation is no longer running a sprint but rather a marathon when it comes to homeland security as other legitimate funding priorities must be addressed throughout the federal government – both inside and outside of homeland security and national defense, and through cross-department support of state and local detection and response capabilities. Investments therefore must be leveraged to achieve protection against major attacks as well as support all-hazards threats, and ensure that sound strategies are aligned for long-term, sustainable success. There must be a strong element of risk management in everything that is done – an open acknowledgement that scarce resources mean making trade-offs and addressing the biggest and most significant problems first.

The United States is a relatively open country with porous borders, autonomous states and a highly mobile society. These characteristics have contributed significantly to the nation's economic well-being and way of life. They are also the features which make the United States particularly vulnerable to a bio-terrorism attack or naturally occurring pandemic. For example, for inhalation anthrax the average incubation period is 7 to 10 days. The incubation period for smallpox is 7 to 14 days and the vaccine is effective only if given within four days of infection. Clearly, with that amount of available time, terrorists not only could infect thousands but, by taking advantage of a highly mobile society, could create an environment in which those thousands infect millions. The time available to provide medical care is often a few hours or even minutes. Antibiotics and prophylactic measures are most effective when provided soon after infection or chemical contamination.

Under the current biological threat detection and warning system, such an attack would be well underway before the first indicators of disease were recognized. By the time response measures were initiated the problem could be extensive. Moreover, the opportunity to remediate the effects of a biological event would be far less than would be the case with a highly responsive detection and warning system.

Chemical agents do not possess the infectious properties of biological weapons. The effects of toxic chemicals and even more importantly, chemical weapons such as nerve gas, will be felt immediately. Therefore, chemical detection and warning systems serve a different purpose than for biological threats, reflecting the concept of operations required for first responders – law enforcement, fire fighters and emergency medical teams – in the event of a chemical event. Chemical sensor systems are useful for safeguarding first responders and civilians who might otherwise enter a contaminated area. A sensor system that can identify the specific chemical agent can also help first responders select appropriate protective and remediation measures.

Detection equipment is also essential to consequence management. These sensors are necessary to determine evolving post-attack downwind hazard/exclusion areas, monitor health care facilities for the spread of contagion/infectious pathogen hazards from re-aerosolization/re-suspension of the agent and ensure the success of recovery/decontamination operations.

Unless there is a desire to radically restructure American society – i.e., curtailing freedom of movement – a warning and detection system needs to be put in place that reflects the two dominant realities of the situation: the mobility of American society and the incubation periods for biological agents of concern. One of the most critical pieces in the process of protecting innocent lives lies with the fast, accurate and dependable detection of biological threats. Specifically, the nation must be able to sample and test the air in areas such as subways, air and sea ports, sporting events, and a multitude of other densely populated locations simultaneously and persistently. Such sampling and testing will provide ample warning of any possible contamination, minimize human-to-human transmission of a contagious agent, reduce the number of victims of exposure to both chemical and biological events and provide timely treatment for those who have been affected.

We must also be able to better protect the first responder community by ensuring response forces not only know that an event has happened, but also have faster and more reliable estimates of the exposure involved, fall-out patterns and appropriate response procedures tailored to the specifics of the event. This is especially crucial when a decision must be made between containment of the scene and evacuation of affected persons for further observation versus immediate mass treatment. Perhaps most significantly, in select chemical and biological events time-to-treatment is often the determinant factor for the survival of victims. Delayed treatment can result in substantially higher mortality rates, and yet with many biological events the onset of symptoms resulting from exposure occurs only after several days. Decontamination of affected areas can take weeks or even months, potentially rendering key elements of the nation's infrastructure inaccessible. The economic effects would be profound.

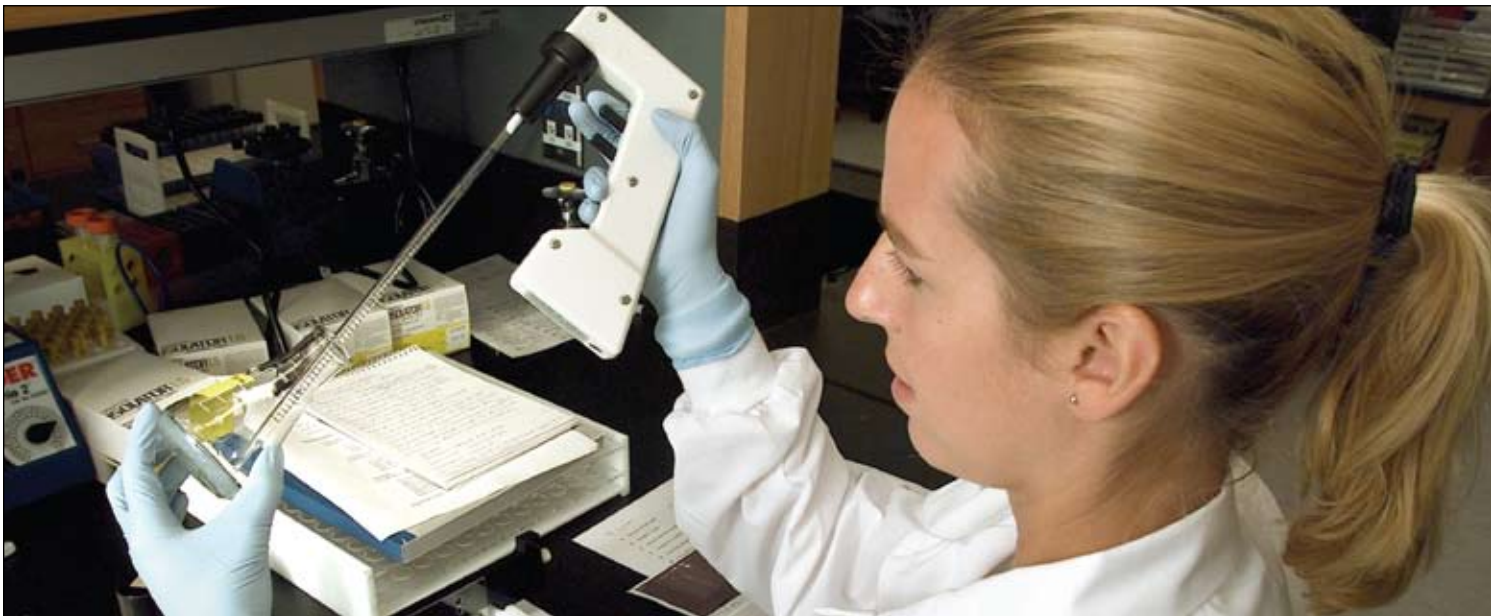
The nation is investing heavily in the capabilities needed to respond to possible chemical or biological incidents. Every state and community has developed preparedness and response plans. The Department of Homeland Security (DHS) is funding extensive training activities and exercises, some such as the TOPOFF series include multiple modes of attack and involve several states simultaneously. Efforts are underway to strengthen the ability of public health systems to handle a wide range of events.

Having already invested some \$50 billion in chemical and biological defense capabilities since 9/11, what is now needed is a smart, network-centric system-of-systems that can tie together the information resources for early warning, agent/threat classification, rapid alert, asset allocation and deployment, assured communications and seamless notification of appropriate and relevant authorities. Early detection and threat classification systems are only a part of the whole – a whole which necessarily involves a multitude of cross-agency investments in everything from interoperable communications, to expansion of federal/state/local emergency response teams, to better personal protective equipment for state and local first responders. This is why the vast majority of the \$50 billion has been spent on response activities and increasing the breadth and depth of the medical countermeasures that are available in the communities and through the Strategic National Stockpile (SNS), and these were necessary and generally prudent expenditures. But the persistent unmet need is early detection, and the opportunity to improve the very alert and warning system that can be seen as the trigger for deployment of those same resources from the Centers for Disease Control (CDC), SNS and others.

The nation's current solution for persistent surveillance against biological threats is the second generation of the BioWatch program. This program is a critical component of the nation's biological preparedness because it helps create a comprehensive interagency surveillance system that can expedite identification of pathogens or other agents in order to facilitate an appropriate government response. The third generation of BioWatch networked defensive sensors is currently being developed and tested; it promises substantially improved performance and reliability in meeting these significant and persistent challenges. Generation 3 also presents the opportunity to finally create sustainable and lasting solutions. Specifically, the mostly manual Generation 2 systems have filters which are removed by hand and then taken to a laboratory for testing, a process that can take from 10 to 34 hours. Generation 3 will possess a number of specific advantages over its predecessor:

- More rapid detection, identification and warning (four hours or less);
- Detection of a larger number of pathogens;
- Wireless communication of detection and warning reports; and
- Lower manpower requirements.

The current biological detection system requires a labor-intensive and costly laboratory process.



Generation 3 BioWatch sensors are in many ways merely the next step in the application of information technology to the field of medicine. Whether it is machines that automatically and rapidly test samples of bodily fluids, portable emergency defibrillators, special screening devices such as CAT and MRI machines, or electronic record keeping, the field of medicine is undergoing a rapid and revolutionary transformation. Information technology serves primarily to reduce the most labor-intensive aspects of the practice of medicine, improve the speed at which data can be collected and analyzed and enhance the effectiveness of diagnosis and treatment.



HOMELAND SECURITY MEANS MANAGING RISK

Risk management as a means of resource allocation is perhaps the single most fundamental concept underpinning the United States' approach to homeland security. This understanding is at the core of its homeland security efforts, from the establishment of DHS to aviation security and investments in everything from intelligence assets to the SNS. Because risk is defined in the 2007 *National Strategy for Homeland Security* as a function of **threat**, **vulnerability** and **consequence**, managing risk through a reduction in any of these three factors inherently reduces the overall risk to the nation.

"Homeland Security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."

- National Strategy for Homeland Security, 2007

Today, the federal government continues to invest heavily in military and intelligence capabilities to address various aspects of the **threat**, be it identification of "persons of interest," ongoing military engagements in Iraq and Afghanistan, or work with allied nations on reducing terrorist access to weapons of mass destruction (WMD). Similarly, DHS, the Federal Bureau of Investigation (FBI), state and local law enforcement, and many other agencies work around the clock to secure the nation's borders, track illicit cargo and maintain a watchful eye on a vast array of current threat streams. This broad set of pre-event activities constitutes the outermost layer in the effort to secure the nation.

The second factor, reducing **vulnerability**, remains substantially underfunded, even though it was a focal point of much initial effort. Specifically, reducing vulnerability through continuous environmental surveillance and ensuring anomalies can be detected, assessed and acted upon enables a more focused response that significantly curtails the total consequences stemming from any chemical or biological event. For man-made events these same attributes allow law enforcement to begin to track down those responsible. Indeed, reducing vulnerabilities through early detection, threat agent/event characterization, response planning and effective information dissemination offers perhaps the most direct avenue for maximum return on every dollar invested because it can greatly enhance all follow-on response activities.

Finally, and especially in the wake of the devastation of Hurricane Katrina, the nation is spending billions of dollars improving its **consequence management** posture in terms of response and recovery preparedness. This arena involves substantial portions of the activities of the Federal Emergency Management Agency and Health and Human Services, including the SNS and the National Disaster Medical System, to name but a few. Increasing response and recovery assets is a cornerstone of risk management, but given the massive scale and scope required it often comes at a heavy price.



REALITIES OF THE THREAT

Despite the media and general public's preoccupation with nuclear and radiological threats, when it comes to terrorist use of WMD the best available analysis indicates that chemical and biological weapons represent the more likely and worrisome means of attack. This is because chemical weapons are the easiest to build and/or acquire, and effective transport and dispersal are not technically complex; while biological weapons can be so inherently deadly and have such long latency periods, during which time they could be spread far and wide, that their use would likely prove the most lethal.

At the same time, there is a growing concern in the medical community about the potential for another global pandemic influenza akin to the naturally-occurring 1918 outbreak that killed tens of millions of people across the world. This is especially true in light of the avian flu radiating outward from Asia over the past several years. The impact of such an event on the nation would be nothing short of catastrophic. Emergency rooms would be overrun, essential services would grind to a halt and the nation's recovery would be measured in years as the survivors worked to recreate the workforce and training needed to restart the economy. Less deadly but economically devastating issues also include an array of naturally-occurring and man-made events affecting agriculture which would, in turn, have a significant impact upon the national food supply.

"Terrorists have declared their intention to acquire and use weapons of mass destruction (WMD) to inflict catastrophic attacks against the United States and our allies, partners, and other interests."

- National Strategy for Homeland Security, 2007

It is possible to build chemical and biological weapons from materials readily available throughout the U.S. The essential equipment needed to create a biological weapon – the culture medium, incubators and drying equipment – are readily available, both new and used, even in the United States. There may be little need for terrorists to risk shipping material across international borders, resulting in less chance of their detection by customs or other agents. For this reason, environmental surveillance systems would in effect become the first layer of defense, a sort of technological tripwire that could enable rapid detection, early warning and an organized response.



A chemical or biological incident could occur with little or no warning.

KEY FACETS OF CHEMICAL AND BIOLOGICAL EARLY WARNING SYSTEMS

The three primary attributes of any comprehensive approach to risk management in terms of detecting chemical and biological agents is that the deployed systems must be **rapid**, **reliable** and **robust**. Each of these facets is critical because the costs of an unrecognized chemical contamination or an uncontained biological outbreak could include unnecessary deaths, massive public disorder, and the swamping of much needed and short-supply medical assets – not to mention prolonged and increasingly severe economic effects. Delays may also mean that the wrong course of action will be taken in terms of the most effective response, and also that law enforcement will not have enough knowledge about the incident to effectively identify and bring to justice the perpetrators, who may go free or – even worse – have time to carry out additional attacks.

- **Rapid** detection of multiple threat agents is the first priority because in the event of an actual attack, minutes and even seconds can translate into the difference between thousands of lives being saved or lost. Rapid identification of an attack enables more effective treatment and appropriate quarantine of any affected areas, while many of the most worrisome biological agents have latency periods during which the infected could unwittingly spread deadly contagions through casual contact.
- **Reliable** detection is similarly critical because the failure to recognize an event has taken place would negate the investment in early warning systems and fail to enable the first responder community to fully mobilize in time to properly respond to the event. At the same time, reliability also includes minimal “false-positives” because inaccurate readings can lead to substantial unnecessary expense as well as “threat fatigue” and diminished public response to reported threats.
- **Robustness** of any deployed system is also critical because the real world presents many challenges more severe than laboratory conditions and, given the number of locations requiring systems, overall operations and maintenance costs are an important factor. This is all the more true because the reality is that an attack may never come or only occur at some time in the relatively distant future. Therefore, a robust system that can withstand the elements and maintain operational effectiveness over time is a key factor in appropriately investing scarce homeland security resources. It also relates to the need to have systems deployed in all manner of potential targets – not just select areas within select cities, but also for smaller cities and agricultural supplies.

SUSPECTED CHEM-BIO WEAPONS OF INTEREST TO AL QAIDA AND ITS AFFILIATES	
Chemical	Biological
Chlorine, mustard gas, phosgene, various nerve agents, cyanide and aerosolized toxic industrial chemicals	Anthrax, plague, smallpox, tularemia, ebola and toxins such as Ricin or staphylococcal enterotoxin B (SEB)

Chemical threats present a specific and immediate danger to the American public as well as to first responders. Chemical agents and their precursors are widely available and are known to have been used by terrorist groups across the globe, perhaps most famously by the Japanese cult *Aum Shinrikyo*, which attacked civilians aboard Tokyo subway trains with Sarin nerve gas in 1995. Chemical agents also are reported to have been found inside improvised explosive devices in Iraq, a sign that the technical know-how for their production and use is spreading.

The requirements and challenges to the detection and monitoring of chemical weapons threats are substantially different than those for biological weapons. The effects of chemical agents will be experienced almost immediately; there is virtually no latency period. In addition, there is very little risk of transmission of agents from one person to another. While very small amounts of chemical weapons can incapacitate or kill an individual, relatively large quantities of such agents or toxic chemicals are required to cause mass casualties. As a result, the primary threat from chemical weapons is to confined areas and especially large gathering places, including many locations within densely populated areas. Rapid and reliable detection at the onset of any chemical event, as well as persistent monitoring to track changes in atmospheric conditions and dispersal patterns as the event unfolds, would clearly enhance local response capabilities. In the event of an outdoor release of a chemical weapon, standoff detection for chemical agent releases could be more effective than point detection because it permits monitoring of a much larger area with greater resolution and with fewer numbers of sensors.

Beyond terrorism concerns, DHS also has identified 13 toxic industrial chemicals of particular concern because of the level of threat they pose. Transportation throughout the country is a major threat for attack or accidental releases. In response, the department has developed plume models for how these chemicals would disperse into the air for the top 100 cities in the U.S. over a 24-hour period in order to determine how much of the population would be at risk. An environmental monitoring system that would provide data with which to confirm the presence of toxic chemicals, track dispersal patterns and collect specific data of use to first responders and law enforcement has obvious utility.

With respect to biological agents the outlook is even grimmer than is the case with chemical weapons. It is widely believed that former Soviet Union scientists in search of work have been recruited by groups affiliated with al Qaida, and intelligence out of Pakistan also confirms an abiding terrorist interest in such weapons. Significant further cause for concern stems from the fact that U.S. and Coalition military forces found direct evidence of al Qaida research into biological weapons during operations in Afghanistan in 2001 and 2002. Although later

analysis concluded the programs were relatively rudimentary at that time, one must consider what advances could have been made in the intervening years. The chief impediment to producing a biological weapon is obtaining the agent seed stock/culture; once these cultures are in hand, production of a biological weapon becomes, in some cases, easier to achieve than chemical weapon production. Open source information suggests that over 40,000 highly trained microbiologists and other scientists are on the “market.” Indeed, as the Pentagon’s Defense Sciences Board reported as far back as June of 2001, “...major impediments to the development of biological weapons – strain availability, weaponization technology, and delivery technology – have been largely eliminated in the last decade by the rapid, global spread of biotechnology.”

Similarly, Mr. Robert Hooks, DHS Deputy Assistant Secretary for WMD and Biodefense, recently testified before Congress, stating:

The challenges we face in assessing current terrorist capabilities and identifying plots make it unlikely that we will receive actionable, specific warning of an impending bioterrorist attack. Furthermore, many of these deadly biological agents are accessible in nature, relatively easy to procure, develop and transport without an advanced background in the biological sciences. Unlike nuclear weapons, few people with advanced laboratory knowledge in the biological sciences are needed to weaponize many of these deadly pathogens. As such, it is incredibly difficult to predict and prevent a biological attack from taking place.

What makes this matter of timely detection and warning all the more pressing with biological threats is that they involve an asymptomatic period during which victims unwittingly could spread the deadly causative agents to other innocents. This creates the potential for cascading cross-contamination to spiral out of control before the first victims even become symptomatic. Introducing biological agents into densely trafficked areas such as airports, subways or at large gatherings could create an enormous catastrophe, one that is a race against time. An effective and reliable network of sensors could serve as the “starting gun” that would, at least, let the federal, state and local response community know that the race against the clock has begun.

Effectively dealing with the risks posed by chemical and biological weapons requires a broad-based approach drawing on resources from all levels of government and the public at-large. One critical but currently insufficient piece of this puzzle is a system-of-systems offering a comprehensive ability to conduct continual environmental monitoring and to assess any anomalies as quickly as technologically feasible. Significantly, such a system lies at the natural funnel point of the entire event timeline (Figure 1) because increased effectiveness in terms of immediate threat recognition and characterization can better align scarce follow-on response resources. The impact such a system can make is literally the difference between life and death. For, if fully capable, it should be able to sound a warning that includes positive identification and density data on the threat agent. This, in turn, dictates recommended first

responder tactics, techniques and procedures, the level of required personal protective equipment and estimates of affected population centers from projected plume movements based on weather data.

Because chemical and biological agents have such different characteristics, the roles of detection and warning systems for each threat will also be different. The effects of chemical agents will be experienced almost immediately and the area of impact will inevitably be local. Chemical agent sensors are useful largely to first responders in the immediate aftermath of the event. Because of the greater latency period for biological agents and the potential for rapid and widespread transmission, biological sensors have their greatest utility in limiting the dispersion of the agent. For both classes of agents, sensors that can rapidly identify the specific type of threat would be useful.

DHS currently has an approved set of chemical threat detection sensors. Most of these systems have their origins in military-grade hardware designed for a different purpose. The majority of these sensors only provide local detection and lack the ability for remote reporting of incidents. Stand-off chemical detectors using infrared and laser techniques are entering the market. Their primary utility is the detection and characterization of outdoor chemical incidents.

Although work remains to be done to improve the effectiveness of chemical threat sensors, the greatest need is for improved biological sensors. The next generation of biological threat sensors will need to be more sensitive and capable of autonomous screening to include both pathogen detection and identification of multiple threat agents such as bacteria, spores, viruses and toxins. The ideal system also would be much less labor intensive, requiring substantially less direct involvement for routine operations, including the initial screening for threat agents. Additionally, it would be able to communicate securely and wirelessly in real- or near-real-time with all relevant parties such as law enforcement, public health officials, state and local medical communities and others as appropriate.

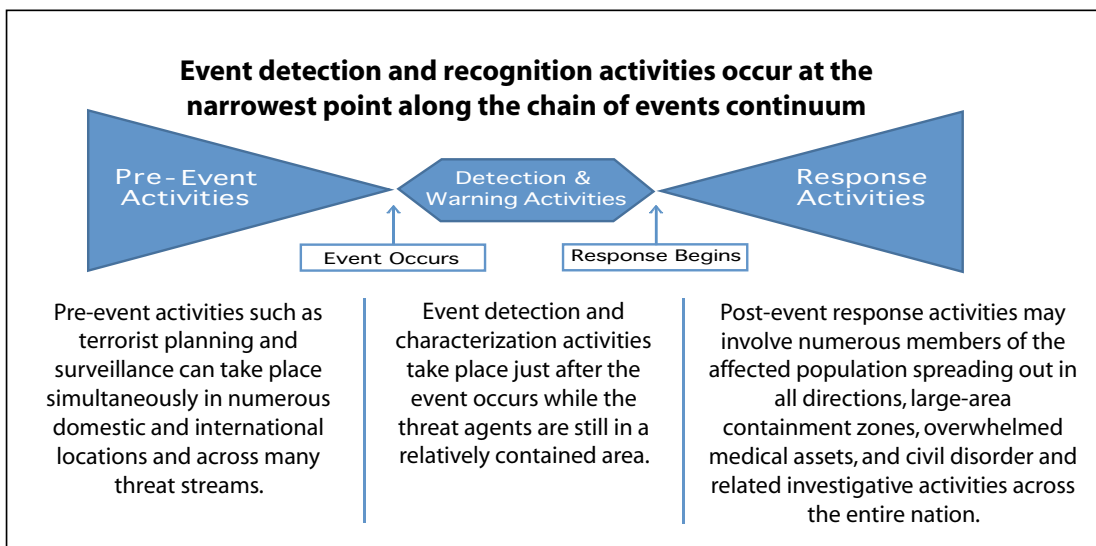


Figure 1.



THE BIOWATCH SYSTEM: CURRENT CAPABILITIES

The first line of defense in the nation's current biological surveillance and detection effort is BioWatch, an early warning system for detecting aerosolized pathogen release. It is currently being used to monitor the presence of airborne pathogens in more than 30 large urban environments. The system was initially deployed in 2003 to detect airborne biological agents and provide early warning of any pathogen release to the local, state and federal agencies responsible for medical response, containment and incident investigation.

In practice, the BioWatch program is comprised of three main elements: sampling, analysis and response. Although initially managed by DHS Science and Technology Directorate, program oversight recently transferred to DHS Office of Health Affairs. Operationally, the Environmental Protection Agency has primary responsibility for maintaining the sensors that collect airborne particles. The CDC coordinates the analysis of samples through state and local public health laboratories. In 1999, the CDC established the Laboratory Response Network. Its purpose is to run a network of 140 state and local public health, veterinary, military and international labs. The FBI serves as the lead agency for the law enforcement response to bioterrorism events. Coordinating these disparate parts has proven a continuing challenge, although a 2007 report from the DHS Inspector General did find substantial improvements over time with effective new procedures in place.

The additional warning provided by the BioWatch program will only be useful if the recipients possess the necessary training. Responders need to be trained to understand both what they are seeing and the information that they are receiving.

DHS' GOALS FOR BIOWATCH

- Early detection and characterization of biological attacks against the nation's cities, high value assets, and mass gatherings to allow for the rapid distribution of life-saving countermeasures.
- Cost-effectively improving bio-aerosol threat monitoring capability and increasing its capacity to cover a greater portion of the general population.
- Providing operational and consequence management guidance and assistance to federal, state, local and tribal entities.
- Integrating BioWatch capabilities into a national bio-threat monitoring and response system.

Two significant common denominators for all the threats discussed above – be they natural or man-made, chemical or biological – are that timeliness matters and knowledge is power. First, the amount of time from event beginning to its being detected and properly characterized is essential. In many of the direst cases the number of lives saved is directly related to the rapid provision of appropriate medical care. Essentially, such care cannot occur until after there is awareness and public health notification of an ongoing event. Similarly, medical and law enforcement authorities must have the knowledge they need – such as the initial point of

detection, time of release, wind direction and other factors – in order to most ably characterize an event as being caused by nature, negligence or malice and, in the latter case, to implement quarantine and prophylactic measures, and find those responsible before they strike again.

Today's BioWatch samplers collect airborne particles, including bacteria and viral particles, onto solid filters using a vacuum system. Its filters are collected manually every 24 hours and transported for analysis to state and local public health laboratories that participate in the CDC's Laboratory Response Network. This is a labor-intensive (and therefore very expensive) approach to a nationwide surveillance system. Even though BioWatch is still much faster than waiting for victims of a biological event to become symptomatic and be treated within local hospital systems, much precious time is lost in the current manual process of collection and analysis.

Operationally, BioWatch worked as designed in October, 2005 on the mall in Washington, DC when it detected trace amounts of *Francisella tularensis*, the bacterium that causes tularemia and which could form the basis of a biological event. Though later deemed to be present at levels not harmful to humans and likely from natural sources, the detection was made over the same weekend that tens of thousands of people visited the mall to attend a large rally. If the bacterium had been present in higher levels it could have been a significant threat to public health, and the first anyone could have known of it without BioWatch would have been 72 to 96 hours post-exposure, when the first victims became symptomatic and sought treatment at local hospitals.

While certainly not perfect, most of the current concerns regarding BioWatch – including operating costs associated with manual processing, human error and analytical speed of test results – are a product of the current system's design, but do not negate the validity or necessity of the mission. Fortunately, technological advancements appear to be near at hand in the form of automated systems that require less maintenance and can serve as their own initial screen for testing the presence of certain suspect particles.

BioWatch should be understood as being but the first line of defense in a comprehensive system designed to provide multiple sources of threat detection, characterization and response. An equally important program is BioSense. This is a national program run by the CDC to exploit existing reporting chains and available healthcare data to improve the nation's capabilities for conducting real-time biosurveillance. BioWatch could provide a tripwire sensor capability that would alert BioSense participants to review existing community medical data and expand reporting activities. Together these two programs could dramatically alter the prospects for the rapid detection, containment and treatment of a disease outbreak.

A Generation 2 BioWatch unit.





BETTER RISK MANAGEMENT: THE NEXT GENERATION OF SYSTEMS

The current generation of biosensors leaves much to be desired. The sensors may not be able to detect small-scale pathogen releases. The limited number of air samplers are not well sited for biological agent detection. Further, the Environmental Protection Agency has failed to ensure proper upkeep of aerosol sampling equipment. There are reports of significant quality control problems often due to the improper handling and transfer of air filters. Remember that the current system requires the manual extraction of air filters and their transportation to an approved laboratory for analysis.

“The challenge of detecting an invisible footprint of an impending bioterrorist plot and preventing an attack or the emergence of a pandemic is daunting. That is why DHS is taking the approach of enhancing early detection systems and building a national biosurveillance capability for situational awareness - to prevent a biological event from becoming a Nation-changing catastrophic event.”

- Mr. Robert Hooks, DHS Deputy Assistant Secretary for WMD and Biodefense, Testimony to Congress, July 16, 2008

DHS's strategy is to improve the sensitivity of its biological detectors while moving to increasingly rapid detection and warning. The current generation of biological threat sensors provides 24-36 hours for detection and warning because they require laboratory analysis. DHS would like to move to a Generation 3 system, one that automatically collects samples, analyzes for the presence of a broader range of threat agents and will instantly notify authorities if it determines that an agent is harmful or otherwise suspect. This system, called the Bioagent Autonomous Networked Detector (BAND) must be capable of aerosol collection, molecular analysis and the identification of bacteria, toxins and viruses, as well as archiving each sample collected for confirmation and forensic analyses.

The Generation 3 detectors are expected to cost considerably less than the current systems. With a goal of \$80,000 to \$90,000 per unit and yearly operation and maintenance costs of \$12,000 to \$41,000, Generation 3 systems will cost some 60-70 percent less to operate than the current Generation 2 systems (which, as noted above, are mostly manual and therefore highly labor intensive). It is hoped that Generation 3 systems will operate continuously for a 30-day cycle before maintenance is required. As a result of such efficiencies and savings, with the deployment of the Generation 3 system it will finally be feasible to use large numbers of sensors to create a web wide enough to offer substantial protection to the population. With the first systems slated for pilot tests during fiscal year 2008, the new systems could begin to be deployed as early as 2009.

But it may take several years before a Generation 3 system is available. In the meantime, an alternative exists, dubbed Generation 2.5, that will provide enhanced capabilities over the current Generation 2 system while Generation 3 technology is fully developed.

The Autonomous Pathogen Detection System (APDS) is equipped to automatically collect samples, analyze them for threat agents, and then remotely notify of a threat. APDS meets most of DHS's requirements for a Generation 3 system. APDS will dramatically shorten the timelines associated with detection and analysis (four to six hours) as well as increase the number of pathogens that can be detected. By utilizing two independent test types, APDS maintains a very low false positive rate, a critical requirement.



THE WAY AHEAD

BioWatch represents just one component of the planned-for broad-based interagency surveillance system able to identify and respond to threat agents, outbreaks or other events. This broader system, the National Biosurveillance Integration System (NBIS), combines data from the BioWatch monitoring systems with reports from CDC and other public health agencies as well as agricultural and veterinary surveillance reports, to create a near-real-time awareness and common operating picture of what is happening across the full panoply of possible threats, be it man-made or natural, biological or chemical.

As called for in the National Biodefense Strategy outlined in Homeland Security Presidential Directive 10 (HSPD-10), NBIS facilitates the early recognition of biological events, including natural disease outbreaks, accidental or intentional use of biological agents, and emergent biohazards. The primary operational component of the NBIS is the National Biosurveillance Integration Center (NBIC), which is charged with:

- Rapidly identifying, characterizing, localizing and tracking any biological event of national concern;
- Integrating and analyzing data relating to human health, animal, plant, food and water; and
- Disseminating alerts and pertinent information.

To accomplish this, the NBIC continuously monitors over 530 information feeds and develops and disseminates a biosurveillance common operating picture, which is a comprehensive electronic depiction with assessments of current biological events, trends and their potential impacts on the nation's homeland security.

Ultimately, the United States needs a more robust system such as that embodied by the concept of the NBIS. However, despite the work of a great many dedicated people and a sizeable investment in biodefenses, at present overall preparedness for a significant chemical or biological event remains relatively rudimentary. Today, given the current system's lag time between an attack and detection, DHS is currently planning to begin testing an interim BioWatch Generation 2.5 that could be deployed to help secure high-risk interior facilities until the Generation 3 systems can be fully vetted, including being properly ruggedized for all-weather use. Such a "2.5" system would be capable of four to six hour warning times, a dramatic improvement over the current 10-34 hour cycles. However, the automated capabilities embedded in Generation 3 are absolutely vital as a first line of attack warning.



Current chemical-biological detection capabilities are inadequate.

The accelerated deployment of Generation 2.5 sensors is an important step on the path towards enhanced homeland security. Further steps will follow. The technologies to support follow-on generations of BioWatch sensors must be pursued. In addition, DHS should consider the advisability and feasibility of building integrated chemical and biological sensors, particularly for highly trafficked locations.

In order to leverage the full value of information technologies, changes in the medical response policies that are in place through the Public Health system will be required. Failure to do so will diminish the effectiveness of the automated early warning capabilities. The potential for earlier detection and identification of biological threats need to be reflected in exercises and planned interoperability training.

The BioWatch aerosol collection systems are just one component of environmental monitoring that complements clinical medical reporting, surveillance

of patterns among patients at hospitals, food and agriculture monitoring, veterinary surveillance and examining the mail. But they are an essential piece because if effectively deployed they sound the alarm that triggers all follow-on activities, and do so while ensuring a better common operating picture of the threat. This will translate into a more effective and more efficient overall response. The end result of a nationwide investment in such a system is that the homeland will be more secure against a wider variety of threats, and in turn will be better positioned to dramatically reduce the overall impact of any future events. In its most basic form, this means that dollars wisely spent today will translate into lives saved and a significant reduction of economic repercussions in the event of any future chemical or biological event. Given the enormity of the potential threat, and the fact that a means of securing the nation must be found that is consistent with its fundamental respect for civil liberties, investment in systems capable of actively monitoring the environment to detect anomalies and possible attacks represents a sound investment pathway.

Biosensors would be useful in other situations, as well. With the 2001 anthrax attacks in mind, DHS should consider using biosensors to maintain control of select agents used in research. DHS also should consider incorporating biosensors into the food processing chain. Recent outbreaks of E-coli and other food-borne infections highlight the need for improved safety. Biosensors would detect contaminants in the production and distribution system.

Unlike other aspects of homeland security which can be left to the states, a monitoring system against biological and chemical threats must be built on a nationwide scale.

Early warning systems are difficult to fiscally justify and sustain because they require consistent funding every year whether the threat materializes or not. Operations, maintenance and training of these systems must be sustained or the nation's state of readiness will degrade without notice and the risk of attack will rise.



CONCLUSION

Securing the nation fully against all the conceivable risks posed by terrorism would be an impossible task even with limitless resources. The effort is all the more challenging given competing budgetary and political priorities that inevitably have begun to eclipse certain homeland security initiatives as time passes without additional attacks on the nation. Given this resource-constrained environment, the only reasonable approach is one of risk management, wherein certain forms of risk are accepted while the nation ensures an appropriate allocation of resources to where the most gain can be had against the most pressing risks.

"We also must never lose sight of al-Qaida's persistent desire for weapons of mass destruction, as the group continues to try to acquire and use chemical, biological, radiological, or nuclear material."

- National Strategy for Homeland Security, 2007

And yet, despite significant effort, the nation remains substantially under prepared for dealing with a series of simultaneous chemical attacks or even a single significant biological event, be it man-made or natural. Indeed, as noted expert Dr. Tara O'Toole, Director of the Center for Biosecurity at the University of Pittsburgh Medical Center, testified before the Senate in October of 2007:

Six years after anthrax was mailed to members of the U.S. Congress and to media organizations, the immediacy and potentially strategic significance of the bioweapons threat is not widely appreciated, nor is the country prepared to cope with the consequences of major bioattacks. This is the case in spite of the extensive efforts to improve U.S. biodefense capabilities.

With each passing year that the homeland is spared another devastating attack it becomes all the more important that programs are developed and implemented that will be effective over the long haul – for it is impossible to know whether the next attack or natural disaster will come sooner or later, only that adequate preparation is required. In short, in the post-9/11 world the U.S. cannot claim to be unaware of the all too real threat posed by terrorists seeking to employ chemical, biological, radiological or nuclear weapons in the homeland or of the similar threats posed by nature. Therefore, effective, rational and sustainable investments should be found that strike an appropriate balance between a national level of enhanced security and every additional given expenditure of resources.

Minimizing the impact of any significant mass casualty event begins with awareness that an event has occurred. More to the point, the alarm bells must be accurate, verifiable and actionable. Although it is essential that there be few if any false alarms, the competing priority is that there must be an effective and timely warning in order to best mobilize an effective response – one that by definition will involve multiple agencies at the federal, state and local levels, as well as the private sector and members of the public.

And yet the nation is only as strong as its weakest link. An ineffective or incomplete system would leave the nation as a whole no better prepared, and therefore a balance must be struck between finding the perfect system for point defense needs and one that can be mass-produced and deployed in sufficient numbers to really protect the American public. What is needed is to build upon existing early warning capabilities through a strategic investment in systems that are proving themselves to be effective, efficient and as close to real-time as possible. Specifically, additional production of APDS sensors needs to be fully funded, to include having DHS reprogram additional resources for production preparation and deployment. This would accelerate the national rollout of this system with at least 30 cities covered in the next few years. Only with such systems will the nation be able to more realistically meet and defeat all too likely future challenges.

Rapid threat detection and characterization is but one of a number of critical elements to a national response capability. Other elements of an effective response include:

- End-to-end planning;
- Stockpiling available vaccines and prophylactics;
- Preparing the national medical community to respond to an incident; and
- Developing new countermeasures.

Many of these functions are the responsibility of parts of the government other than DHS. However, without rapid threat detection and characterization, these other efforts are likely to be much less effective in the event of an attack.

Addressing the requirements for effective early warning through an enhanced BioWatch sensor system addresses only part of the problem of defending the homeland against biological threats. Additional work and greater funding is needed to fully exploit the opportunities provided by the BioSense program. Improved sensors for the detection of chemical attacks or toxic spills are also desirable. Beyond these improvements, the nation needs to more seriously plan and prepare to respond to a chemical or biological event. This includes better preparation for first responders, ensuring the availability of vaccines and prophylactics, and training and exercising the response command structure at the national, state and local levels.



PRINTED IN THE UNITED STATES OF AMERICA
NOVEMBER 2008



1600 Wilson Boulevard • Suite 900 • Arlington, Virginia 22209

tel 703.522.5828 • fax 703.522.5837

www.lexingtoninstitute.org • mail@lexingtoninstitute.org