

Biodefense:

Robert J. Clerman



Many in the homeland security community believe that a bio-threat is not a question of if but when.

In the realm of catastrophic terrorism, biological attack is among the most ominous threats we face in the new security landscape of the 21st century. It is also certain to occur. How we confront this threat that is as unthinkable as it is inevitable is a measure of our overall ability to meet the security challenges of our time. Dr. Anthony Fauci, director of the National Institute of Allergy and Infectious Diseases, recently reaffirmed the belief of many in the homeland security community that a biological threat is inevitable: "Those of us who are in the public-health arena generally feel strongly that it isn't a question of whether ... but when." Predictions of a pandemic flu outbreak in the not too distant future are equally ominous. The July/August 2005 issue of *Foreign Affairs* (www.foreignaffairs.org) contains a series of articles about the threat of an

Are We Ready?

avian influenza virus spreading to a pandemic that could kill over 200,000 Americans. Without adequate vaccines and if the strain proves resistant to antifu drugs, that number could grow to over 15 million in the US and over 100 million worldwide. So, whether of natural or nefarious origins, we face a modern manifestation of a mortal threat that has plagued humans over the ages: infectious disease with catastrophic consequences—not just physical but also emotional, as the 2001 anthrax attacks have demonstrated.

Although some would say response efforts to date fall far short, the US *has* expanded funding and developed strategies. Attempts have been made to state the national goals—prevent, protect and recover from attacks—and outline the means to attain them—create sensor networks, develop incentives for prophylactic drug development, and establish health-surveillance programs. And despite the ups and downs of particular budgets, the race is on to do even more. BioShield I, passed in 2004 to fund the procurement of medical countermeasures, such as vaccines, will soon be joined by BioShield II, which aims to create incentives and take down barriers to industry producing countermeasures. BioWatch, the program to install pathogen sensors in cities, is expanding the number of participating cities. Health facilities around the country are testing dozens of biosurveillance programs to detect early indicators of disease outbreaks, and another “Bio” initiative, BioSense, seeks to tie them together.

Despite this progress, sizable obstacles remain, even in the newer biodefense strategies. The articles in this issue of *Sigma* take a close look at the technological and organizational changes we must make to hone our national response to a biological threat, as well as the formidable challenges that remain.

Fiscal responsibility

After the anthrax attacks of 2001, no one could argue that a biological threat was theoretical, and the SARS outbreak a few years later transformed a discussion of emerging infectious diseases into worldwide mobilization. The US responded by opening its checkbook. Civilian funding for biodefense grew nearly twentyfold from 2001 to 2005, with expenditures going toward revitalizing the long-neglected public-health infrastructure, expanding

systems for early warning and response to disease outbreaks and developing vaccines and other countermeasures in biodefense. Now the public-health sector, long accustomed to orphan status at budget time, complains bitterly when double-digit rates of funding growth are questioned.

And some in Congress and elsewhere *are* questioning. They want to know what’s been achieved so far and what’s left to do, and they’re reluctant to continue that funding without answers. Their reaction is in part a natural desire to support more visible and popular expenditures. And were this simply a political debate over spending, one of many in legislatures around the country, it would be of no special concern.

But are the politicians mirroring a growing complacency in the public at large? As the September 11 attacks and the ensuing anthrax discovery become less immediate, other priorities, such as education and medical costs, rise to the top. Has the initial visceral reaction given way to doubt, possibly even skepticism?

Given the haphazard execution of biodefense funding, impatience and wavering commitment are hardly a surprise. It is understandable that, given the crisis atmosphere post 9/11, funding began with no clear integrating strategy, and without it, disparate programs—ones that could be working toward a common goal—now compete for resources. Moreover, because no single expenditure can be measured in terms of its contribution to the overall national capability, it is evaluated individually (if at all). Consequently, any policy benchmarks are parochial and short-term.

To more tightly manage this scattered collection of programs, the Bush administration completed a comprehensive review of biodefense capabilities. In “Biodefense for the 21st Century” (www.whitehouse.gov/homeland/20040430.html), administration leaders point to expenditures and accomplishments across a spectrum from global efforts to deter biological weapons proliferation to research on new vaccines and therapies, to systems for detecting biological attacks as they occur. As part of this new strategy, they view current and planned activities within a framework that has four pillars: threat awareness, prevention and protection, surveillance and detection, and response and recovery. This framework is applied to a patchwork of programs that span many agencies, committees of Congress and specific functions.

Principles of readiness

The new national strategy is a step in the right direction, but it falls short of what's needed. What's needed is a link between strategy and implementation—a mechanism to make wise choices among competing investments in a system context, regardless of the specific agency or funding authority. These choices must be guided by principles that reflect the inherent complexity and uncertainty of the biodefense mission. The first principle is that no one strategy, system, or technology will eliminate the threat, and a strategy that aims to reduce and manage risk calls for a layered solution. The second is that time is of the essence—our ability to survive a biological outbreak will be determined in large part by our ability to gain early warning and intervene to protect target populations. Third, the integration of both capabilities and players is essential to a coordinated response.

This issue of *Sigma* examines readiness in light of these three principles. In “Connecting Goals and Means,” I examine the strategic context of layered defense, the critical importance of early warning and coordinated response, and the need for a program architecture to guide investment and make it easier to integrate capabilities. This article sets the stage for the rest of the issue, which covers the key areas of surveillance and attack detection, and capacity planning for the surge of people that would require medical attention after exposure.

In “Present Practice, Future Goals” David Roberts explores the status and potential for syndromic surveillance systems—continuously monitoring aggregate clinically related data, such as patient encounters with the health system, to detect disease outbreaks. Early identification of outbreak indicators can buy valuable time for public-health and law-enforcement officials to investigate and respond accordingly.

In “Instrumentation, Innovation, and Implementation” James Buthod and Robert Taylor explore how detectors might play a role in the early warning of a biological threat agent's release. Detection must be accurate and timely enough to allow public-health and law-enforcement officials to implement a response plan and minimize mortality and morbidity through early intervention. Developing a more effective, systems-wide detection approach requires specific technical and process enhancements, such as smaller units and increased automation to reduce sampling overhead.

Fred Cecere and Clement McGowan continue the theme of coordinated planning in the face of uncertainty in “Intelligent Surge Capacity Planning.” Under worst case scenarios, local, state and federal authorities must plan for the ability to treat unprecedented numbers of victims in a timely and efficient manner to minimize the mortality and morbidity associated with an event. By viewing surge capacity as a system, planners can apply principles such as supply-chain management to replenish resources and model scenarios to study the impact of various agents and treatment modalities, such as quarantine. The authors propose the use of an event taxonomy that serves as the basis for a playbook of event scenarios in much the same way as meteorologists use taxonomies to classify the devastation that meteorological events can cause.

In some cases, existing capability can be put to use in a surge

situation arising from a biological event. In “Virtual Support Through Clinical Call Centers,” Birdie D'Andrea suggests that the technology and care-delivery model that disease-management organizations now use is well suited as a basis for virtual triage, clinical information, and emotional support to patients and the “worried well.” Such virtual support is another option in increasing our surge capacity.

Opening a dialogue

The articles in this issue of *Sigma* address key elements of how to move the country forward to meet the threat of biological attack and natural disease outbreak. The insights offered are beyond simple critiques of specific technologies or systems. They are aimed at opening a dialogue on building a national capability—one built on the best traditions of military systems, the lessons learned from civil systems, and the extensive knowledge and capability that we have already accumulated about how to protect our homeland from a biological threat. Creating a comprehensive, integrated biodefense capability across the nation is a prodigious task. Our intent in this issue is to examine what has been done and what could be done to more systematically approach biodefense planning. Each article addresses a critical component of a layered biodefense strategy, providing the reader with an overview of the current status, gaps, and recommended next steps, all in an effort to move our country to a greater state of readiness.

Finally, although our focus is on a planned terrorist attack on the US, the insights also apply to planning for any event with potential for widespread mortality and morbidity, such as pandemic influenza. The threat to life and infrastructure is the same whether intentional or natural. Both warrant more than a passing thought. Forewarned is forearmed, and not planning accordingly and with some urgency will be deadly. ❖



Robert J. Clerman is vice president for Corporate Mission Initiatives at Mitretek. For more than a decade he has focused on homeland security, including leading early efforts in agricultural security and critical infrastructure protection, developing a strategic plan for biodefense, and developing strategies and best practices in biosurveillance and medical preparedness. He earned master's degrees in environmental science from the University of Virginia and in computer science from Johns Hopkins University. Contact him at rclerman@mitretek.org.