Center for Biosecurity

UPMC | University of Pittsburgh Medical Center

621 E. Pratt Street, Suite 210, Baltimore, MD 21202 | phone (443) 573-3304 • fax (443) 573-3305

"Hearing on Bioterrorism Preparedness and the Role of DHS Chief Medical Officer"

Testimony of Tara O'Toole, MD, MPH, Director and CEO, Center for Biosecurity of UPMC

Congress of the United States, U.S. House of Representatives Committee on Appropriations, Subcommittee on Homeland Security, March 29, 2007.

Mr. Chairman, Congressman Rogers, and members of the Committee, thank you for the opportunity to address the vital issue of biodefense and the difficult challenges surrounding the U.S. government's efforts to protect civilians against bioattacks.

My name is Tara O'Toole. I am the Director and CEO of the Center for Biosecurity of the University of Pittsburgh Medical Center and Professor of Medicine at the University of Pittsburgh Medical School. The Center for Biosecurity is a nonprofit, multidisciplinary organization located in Baltimore which includes physicians, public health professionals, and biological and social scientists. The Center is dedicated to understanding the threat of large-scale lethal epidemics due to bioterrorism and to natural causes. My colleagues and I are committed to the development of policies and practices that would help prevent bioterrorist attacks or destabilizing natural epidemics and, should prevention fail, that mitigate the destructive consequences of such events.

This committee, I believe, has a unique opportunity to consider "homeland security" from a strategic perspective. The complexity of "homeland security" missions and the number and diversity of programs and offices within the Department of Homeland Security (DHS) make such strategic thinking very difficult. But it is critically important that the Congress identify those "homeland security" activities and capabilities that are most critical to protecting national security, both for the near term and for the future. This requires that Congress understand the most likely and potentially most destabilizing threats that might arise either from natural causes or from the actions of "a thinking enemy." Wherever possible, we should strive to implement defenses that make the country not only safer, but stronger and more competitive.

Today, I would like to address three issues that I and my colleagues at the Center believe are critical to homeland security:

- First, I will argue that bioterrorist attacks are an urgent and growing threat and that the capacity to mitigate the consequences of such attacks is a top national security priority deserving of more attention and action.
- Second, I will discuss the need to better prepare the country to deal with mass medical casualties in the event of a terrorist attack or natural disaster. More than five years after the anthrax mailings, the U.S. still lacks a coherent plan for conduct of operations to guide the healthcare sector's response to mass casualty care in the event of a bioterrorist attack or other large-scale catastrophe.
- Third, I will urge that DHS initiate a strategic examination of the current state of "biosurveillance" and develop a five-year strategy for biosurveillance in collaboration with other federal agencies and key stakeholders. Although I believe that the current trajectory of biosurveillance is understandable in historical context, I also believe that the country could make different and more useful and cost-effective investments in biosurveillance than are currently planned. Specifically, our analyses indicate that national investments in rapid diagnostic tests, electronic health records, and digital links between hospitals and public health agencies will yield more benefits than will additional investments in environmental sensors or syndromic surveillance technologies.

Bioterrorism is an Urgent and Growing National Security Threat

A covert bioterror attack on U.S. civilians or, even worse, a campaign of such attacks, is within the capability of terrorist groups today and could potentially cause tens of thousands of casualties and immense social and economic disruption. The scope and seriousness of the bioterror threat has been emphasized and verified by multiple U.S. government agencies and analyses. DHS' own Probabilistic Threat Assessment of Biological Agents is a well-done technical analysis of the bio-threat. I urge every member of this committee to be briefed on this assessment and to be familiar with the national security implications of this analysis.

The Lethality of Biological and Nuclear Weapons are Comparable

The lethality of biological weapons mirrors that of nuclear weapons. Nothing else—not large conventional explosions, not chemical weapons, and not radiation devices—is in the same class. In 1993, the Congressional Office of Technology Assessment determined that 100 kilograms of aerosolized anthrax released upwind of Washington, DC, under favorable weather conditions would cause 1 to 3 million deaths—approximately the same number of casualties that would result from a one megaton hydrogen bomb dropped on the city. A subsequent analysis by the World Health Organization posited similar death tolls from a biological attack.

Biological weapons have been proven to work on a large scale by U.S. testing in the South Pacific in the 1960s and 70s. We know now that the former Soviet Union had a massive bioweapons program that employed 40,000 people at its height and manufactured hundreds of tons of powdered anthrax and smallpox annually. This secret program was largely invisible until defectors detailed its existence.

It is important to recognize that the technical barriers to building bioweapons that faced the superpowers in the 1970s have been overtaken by the rapid advancements in bioscience. There are today no significant technical barriers to terrorists seeking to conduct large-scale bioattacks. As the Defense Science Board wrote in June 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.*
>
> *- Report of the Defense Science Board/Threat Reduction Advisory Committee Task Force on Biological Defense. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. June 2001.*

Biological Terrorism is the National Intelligence Council's "Greatest Concern"

Al Qaeda is known to be seeking biological weapons, and according to the Robb-Silverman Commission's report on WMD Intelligence Capabilities, evidence gathered in Afghanistan demonstrated that Al Qaeda's efforts to develop bioweapons were more advanced than had been expected.[1] In 2004, the U.S. National Intelligence Council declared:

> *Our greatest concern is that terrorists might acquire biological agents, or less likely, a nuclear device, either of which could cause mass casualties.*
>
> *- Mapping the Global Future. Report of the National Intelligence Council's 2020 Project, December 2004.*

The ease with which bioweapons programs can be hidden and the lack of any definitive intelligence "signatures" indicative of illicit bioweapons activity are some of the reasons why these "asymmetric" weapons are attractive to terrorists. The materials and know-how needed to build a powerful bioweapon have legitimate, "dual-use" applications, making it very difficult to identify or track bioterrorist plans and preparations. We cannot count on identifying and interdicting would-be bioterrorists before they strike, and, as the 2001 anthrax attacks demonstrated, it is extremely difficult to assign attribution for such attacks once they occur. This means that traditional deterrence, which rests on certain and severe retribution, might be less effective against bioterrorist threats.

Biodefense Rests on Capacity to Mitigate Consequences of Attack

The extreme difficulty of detecting or interdicting bioterrorist efforts means that defense against covert bioterror attacks must rest on the nation's ability to diminish the death, suffering, and economic and social disruption that could result from bioattacks. This harsh truth is presumably the insight behind the dramatic increase in biodefense spending that began in 2002—federal spending on civilian biodefense went from approximately $250 million in FY2002 to nearly $4 billion in FY2003; funding levels overall have remained more or less constant since. These sums are significant when measured against other spending programs in the Department of Health and Human Services, which presides over most "biodefense" initiatives. Four billion dollars per year does not seem like so much money if one compares this amount to sums routinely spent on national security programs in the Department of Defense. The important questions, of course, are: Is the country getting the defense against bioattacks that we need with the programs we have? Could we do better?

Key Elements of Epidemic Response: Situational Awareness, Care of the Sick, Protection of the Well, Delivery of Countermeasures, and Engagement of the Public

Bioterrorist attacks result in epidemics of infectious disease, which different from the results of other crises or other forms of terrorism. Epidemics have been called "terrorism in slow motion" because they unfold over a period of days and even weeks. It is not immediately clear how big an epidemic is or will become; it may be impossible to discern quickly if there has been a single attack or several. Many questions will confront leaders struggling to manage a bioattack: Who has been infected, who is at risk, where are the needed resources, where are they located now, and how might they be deployed to best effect?

The confusion that inevitably accompanies epidemics—whether they are naturally occurring or the result of a deliberate attack—is not easily resolved. Attaining sufficient "situational awareness" to make informed decisions about what to do will be a major challenge for decision makers at all levels. In the current U.S. healthcare system, it will probably be extremely difficult to even obtain an accurate, near real-time count of infected victims during a bioattack because rapid diagnostic tests and digital connections between public health and hospitals are lacking.

In addition to maintaining situational awareness, the other key epidemic response capabilities include the capacity to care for the sick; the ability to "protect the well"—to prevent contagious diseases from spreading, to immunize the population against future attacks, and to protect infected (but not yet symptomatic) persons; the capacity to deliver effective medical countermeasures (medicines and vaccines); and the capacity to constructively engage the cooperation and collaboration of citizens in epidemic response.

Medical Response to Mass Casualties

The DHS Office of the Chief Medical Officer has proposed taking responsibility to prepare medical response Conduct of Operations ("conops") plans for the major disaster scenarios DHS has judged to be highest priority. In my view, this is a critical task that is long overdue.

The U.S. healthcare delivery sector is not equipped or prepared to provide timely medical care to the tens or possibly even hundreds of thousands of casualties that could result from a successful bioattack. No municipality could care for a sudden flood of even 500 victims with inhalational anthrax—there simply is not enough "surge capacity" in today's financially stressed healthcare system to handle this load. The problem of lack of medical surge capacity is not specific to bioterrorist attacks. Nearly every type of terrorist attack or large-scale natural disaster would impose significant demands on healthcare facilities. At a March 15, 2007, meeting of medical and public health experts sponsored by the White House Homeland Security Council, attendees warned that the U.S. healthcare system would likely "collapse" in such events.

Yet, as we saw in the response to Hurricane Katrina, there is no national doctrine or operational plan that guides how healthcare facilities should prepare for or react to such calamities. Astonishingly, more than five years after high grade anthrax was mailed to members of Congress and the media, there is no conduct of operations plan for how the U.S. health-

care system would cope with the casualties of an anthrax attack. This is the case even though a bioterrorist attack is the mass casualty scenario judged by the National Intelligence Council to be "of greatest concern."

The federal government has not proposed or endorsed a coherent strategy or conduct of operations plan for medical response to mass casualty events, and has not adequately funded even minimal hospital preparedness activities. Responsibility and accountability for medical preparedness and response during large-scale catastrophes within HHS and DHS are unclear, and in both agencies these functions are grossly understaffed and underfunded.

The Department of Health and Human Services (HHS) has provided modest funding for hospital preparedness since 2002, but much of this money has failed to reach hospitals; in any case, the amounts appropriated are small—about the cost of a single nurse's salary per year for each of the 5000-plus hospitals in the country. The Center for Biosecurity has estimated that it would cost at least $5 billion annually (~$1 million per hospital) to prepare hospitals for pandemic flu—this is exclusive of the costs of stockpiling supplies. Dr. Dennis O'Leary, the CEO of the Joint Commission (formerly the Joint Commission on Accreditation of Healthcare Organizations) has stated that $1 million might improve preparedness at a small, 20-bed hospital, but would likely be inadequate for large, urban medical centers, which might require as much as $10 million annually for disaster preparedness.[2]

Interpreting this minimal funding and relative lack of federal guidance as a signal that hospital disaster preparedness is a low priority, many hospitals have conducted only minimal disaster planning. Few hospitals have created regional plans for collaborating with other hospitals in their jurisdiction. Those medical centers that have formed regional planning groups have had difficulty communicating with other regions or spreading lessons learned.

A major problem is the lack of a recognized "organizing authority" with the standing to induce independent, competitive hospitals to engage in joint planning and to collaborate in crises. Most mayors and governors are unaware of the importance of regional hospital collaborations for emergencies in part because the hospital system is largely in private hands and not part of the government, and partly because America has not experienced many "mass casualty events."

These facts make the need for a coherent medical mass casualty response all the more urgent and necessary. Although it would be desirable going forward to clarify the medical response authorities and responsibilities of DHS versus those of HHS, the current pressing need is to produce a coherent, national conduct of operations plan for mass medical casualty events. Such an effort should proceed with a great deal of stakeholder involvement and collaboration. A Mass Casualty Medical Response Conops Plan cannot be successfully created or imposed by the federal government without significant involvement of medical professionals and hospital leaders around the country. Many preparedness efforts underway in some regions are worthy of emulation and provide valuable lessons, as does our experience with medical response during Hurricane Katrina.

Ensuring Adequate Situational Awareness During Epidemics

The first requirement of epidemic management is situational awareness. Making informed leadership decisions and convincing the public to cooperate with official recommendations will depend on obtaining an accurate picture of what is happening and what is possible.

Until recently, most efforts to ensure "situational awareness" during bioterrorist attacks or natural epidemics have centered on efforts to detect an attack or the onset of a disease outbreak. The governing concept is that early detection will enable an earlier response and save lives. This is the premise behind "BioWatch," a DHS program which was deployed in some cities just before U.S. troops entered Iraq in 2003 and which consists of environmental sensors designed to detect specific airborne bioweapons agents.

BioWatch is intended to provide early warning of an aerosolized bioattack. While early warning is desirable, there are a number of practical, operational, and strategic questions that deserve examination before additional investments are committed to the BioWatch program. For example:

- Will the turn-around time for BioWatch samples—the time required to collect samples from the sensors, transport them to labs, and analyze the filters—really shorten the time needed to detect an attack that is large enough to be picked up by the sensors, or will astute clinicians recognize the attack just as quickly?
- Does it make sense to invest limited biodefense funds in more advanced BioWatch technology even as we cut funds for the public health personnel needed to analyze BioWatch data, as we are now doing? Many public health professionals at the March 15 White House meeting noted that assessment of BioWatch data requires use of limited public health resources that might be otherwise employed to greater effect.
- Environmental sensor technologies are now being marketed to individual companies for installation in privately owned buildings. Will DHS develop commercial standards or regulations to ensure that such systems are reliable and maintained properly? Should public health agencies be required to assess every warning signal ("hits") registered by privately owned sensors? Should public health agencies be reimbursed for such assessments?
- Would we improve detection more cost-effectively by focusing on raising clinicians' awareness of bioweapons-related disease or by making investments in point-of-service diagnostic tests, which could not only detect bioweapons agents but also help identify victims once an attack occurs?
- How useful will BioWatch data be in determining the site of the bioweapons release and who was exposed? In previous TOPOFF exercises, dueling "plume models" of both radiological and biological weapons releases caused great confusion.
- Would digital connections between hospitals and public health agencies be more cost-effective and more useful than environmental sensors in detecting natural disease outbreaks and bioattacks? Such connections, which are now rare, would certainly be valuable in ascertaining situational awareness once an epidemic is underway.
- What are the long-term plans for BioWatch deployments? Thinking enemies are likely to learn which jurisdictions are covered by BioWatch and which areas of the country are less thoroughly monitored. BioWatch coverage for the entire nation—which the JASONs calculated in a 2003 report—would cost $40 per person per year[3].

These are complicated questions. I want to acknowledge that DHS personnel have worked extremely hard to deploy BioWatch, to improve its technical performance, and to coordinate response scenarios with local public health officials and first responders. However, I remain skeptical about the overall value of the program.

It is the assessment of the Center for Biosecurity that digital links among hospitals and large HMOs and local public health agencies, and investments in interoperable electronic health records—which authorities agree would improve healthcare quality and lower healthcare costs on a routine basis—would be far more cost-effective than funds spent on future generations of BioWatch.

Most advanced countries have electronic health records—the UK's system, for example, makes it much easier for British hospitals and doctors to communicate in real time during crises such as the London metro bombings. President Bush has advocated the adoption of electronic health records and set a ten-year timeline for establishing such systems, but does not anticipate the federal government providing capital for such efforts. Investments in electronic health records—an electronic health information highway system—is an example of how investments in improved homeland security could render the country safer from devastating bioattacks while simultaneously making the nation stronger on a daily basis.

References

1. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (Robb-Silverman Commission). Report to the President of the United States. March 31, 2005.
2. Drexler M. Interview with Dennis S. O'Leary, MD, President, Joint Commission on Accreditation of Healthcare Organizations. Biosecurity and Bioterrorism. 2006;4(4).
3. JASON. Biodetection Architectures. The Mitre Corporation. February 2003.