

## High-Throughput Laboratories for Homeland and National Security

SCOTT P. LAYNE AND TONY J. BEUGELSDIJK

### AN INCREASING AND LONG-TERM THREAT

IT IS COMMON KNOWLEDGE that compared to nuclear and chemical weapons, biological weapons are much less expensive to produce and use. It costs about \$1 million to kill one person with a nuclear weapon, about \$1,000 to kill one person with a chemical weapon, and about \$1 to kill one person with a biological weapon. The low cost and minimal infrastructure needed to carry out bioattacks suggest that current and future terrorists will pursue this route.

The world has witnessed dictators such as Saddam Hussein with biological weapons of mass destruction, and terrorist networks such as al Qaeda that call for *jihad* and waging asymmetric warfare. To this day, we do not know whether the perpetrator of the post-9/11 anthrax letter attack was an organized “bio bin Ladin” or a lone “bio Kaczynski” but either seems plausible. Because of extensive media coverage, however, we do know that the leaders of rogue nations and terrorist networks see biological attacks in more threatening ways. Conceivably, the post-9/11 anthrax letters may have represented a “test” that surpassed all expectations: It revealed that small bioattacks can overwhelm the public health system and induce ripple effects with enormous social and economic consequences. Worse yet, with current bioagent tracing capabilities, the risk of attribution appears to be small to nil.

Intelligence reports that have been released to the public indicate that nations like Iraq and North Korea possess smallpox and, in all likelihood, in readily spreadable (i.e., weaponized) forms.<sup>1</sup> A few plastic bags of powdered smallpox are easy to conceal and transport and, if released, would be capable of starting major epidemics that

kill vast numbers of people. In the hands of rogue nations or terrorist networks, such materials constitute one of the ultimate weapons of mass destruction and/or instruments of biological blackmail.<sup>2</sup>

As a result, the United States is vaccinating military personnel serving in the Middle East and first responders at home against smallpox. The U.S. Congress is also allocating unprecedented sums of money for bioterrorism-related research, and the new Department of Homeland Security is mobilizing government agencies to work together. As a nation, we are awakening to the “biological genie” and struggling to put it back in the bottle. As we reshape our postures and defenses, new programs that increase our overall security must begin.

The above remarks point to a few inescapable facts. Biological weapons and bioterrorism pose a significant threat to homeland and national security. The threat comes from rogue nations, international terrorist networks, and less sophisticated but still dangerous domestic groups and persons. The primary issue is that the United States must now devise a strategic plan to *prevent*, *deter*, and *respond* to the long-term threats. The plan must take advantage of our best scientific and technical know-how and support public health, homeland security, and national security efforts.

So far, our efforts have focused on improving the care of potential biological victims. Across the country, they involve getting our neglected public health infrastructure, emergency medical services, hospitals, and doctors better prepared for man-made events and natural infectious disease outbreaks. At the same time, however, we must also build new capabilities that can prevent and deter bioattacks and, in case of crisis, help us to save lives. How would these capabilities take shape?

---

Scott P. Layne, MD, is an Associate Professor in the Department of Epidemiology, School of Public Health, University of California, Los Angeles.

Tony J. Beugelsdijk, PhD, MBA, is a staff member in the Industrial Business Development Division, Los Alamos National Laboratory, Los Alamos, New Mexico.

## A NEW VISION FOR BIODEFENSE LABORATORIES

A necessary foundation is a high-throughput infectious disease laboratory and information processing system that relates the molecular fingerprints of bioagents to their sources worldwide. The new system could be easily assembled from existing science and technology in the academic, industrial, and governmental sectors. The program would bring together and integrate various key disciplines, interests, and expertise to deal with the threat of bioterrorism in the most effective ways possible.

The high-throughput laboratory and database system would provide comprehensive analyses of bioagents immediately after attacks. In a time of crisis, it would offer much needed surge capacity to the network of public health laboratories operating throughout the country. Such frontline and back-up capacities would help to save lives by expediting effective remedies and therapies. At the same time, the system would provide swift and accurate identification and attribution for effective action. It would also provide the technological foundation to develop robust national policies to take appropriate actions against enemies of the United States who use or might use biological weapons. Because microbial forensics can determine the origin of bioagents with a high degree of certainty, the laboratory system would have a potential role in counterterrorism and nonproliferation that can be summed up as: *virtually assured detection, attribution, and response (VADAR)*.<sup>3</sup>

The fully operational system would be capable of handling both bacterial and viral agents. Its flexible design would make it easy to augment with new and cost-effective technologies as they become available as well as other technologies that provide more highly discriminating tests. The highly accurate analysis of samples would be accomplished by integrating molecular biology, laboratory automation and robotics, and informatics capabilities into one system.

An extensive collection of samples would be achieved through concerted worldwide effort. The system would also work in conjunction with outbreak investigations and syndromic surveillance efforts. The operating system for the high-throughput laboratory would enable secure access worldwide, allow tests to be carried out in a flexible manner, schedule and perform numerous tests on a routine basis, and deposit test results into bioagent databases. The information in these databases would be organized in ways that facilitate detailed analyses of bioagents, association of fingerprints of one sample with another, and enhanced discovery of new and important distinguishing biological characteristics.

The overall program would produce new technical capabilities through a national and integrated R&D strategy

that will better detect, identify, locate, frustrate, disrupt, and defeat the production and use of biological weapons agents. Such capabilities would operate continuously, provide real-time information, and serve as a biodefense sentinel.

## FOUNDATIONS

The plan to build a new kind of high-throughput laboratory against bioattacks and bioterrorism was first published in 1998.<sup>4</sup> An editorial in the same journal called attention to the plan's importance and called for action.<sup>5</sup> The system would permit scientists to connect to the high-throughput laboratory by way of the Internet or secure intranets. A set of process control tools would then be used to program and manage all the necessary steps, such as the design of tests, documentation of samples, submission of samples, analysis of data, and assignment of data access privileges.<sup>6</sup> Altogether, the system would permit scientists to use the high-throughput laboratory in the same ways that they might use hundreds of skilled technicians. Yet the data would have far fewer errors than is possible with technicians and would also be purely digital and, therefore, easy to retrieve and manipulate by computers.

The initial interest led to a meeting sponsored in part by the Institute of Medicine and the National Academy of Engineering in 1999. As discussed during the meeting and presented in the book *Firepower in the Lab*, all the essential science and technology are available to build a high-throughput laboratory against man-made and naturally occurring infectious disease threats.<sup>7</sup> Before September 11, these foundations helped to shape scientific thinking, but after it they galvanized a broader consensus.

In December 2001, the National Academies established the Science and Technology for Countering Terrorism committee to help the United States develop a science and technology program plan and research strategy for combating terrorism. The committee's first task was to characterize the range of threats to the nation's security by targets, weapons, and delivery systems, and the possible points of intervention. The committee's second task was to develop research agendas in seven areas, including biological threats.

In June 2002, the committee published its comprehensive report, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, and also delivered it to the United States Congress and Office of the President. The report offers many far-reaching recommendations, including ones to build a high-throughput laboratory and information processing system against bioterrorism and to develop and coordinate bioterrorism forensics capabilities.<sup>8</sup>

## AVAILABLE CAPABILITIES, TESTS, AND THEIR APPLICATIONS

The Centers for Disease Control and Prevention (CDC) and the Association of Public Health Laboratories have joined forces to build the nationwide Laboratory Response Network. The members of this network consist of state- and county-based public health laboratories that work together on a three-tier hierarchy. Such organization enables the country to maintain a large number of low-level containment and diagnostic laboratories that can feed progressively into a smaller number of medium- and high-level ones with greater testing capabilities.<sup>9</sup>

During the 2001 anthrax letter attacks, the Laboratory Response Network was called on to process more than 100,000 samples over a one-year period, which significantly challenged its overall capacity. In spite of subsequent and significant investments to enhance it, the overall network still has limited surge capacity and is not digitally interconnected to any great extent. As a result, various laboratories function more like individual nodes within the network and, in the event of a larger or more distributed bioterrorist attack, could be easily overwhelmed by hundreds of thousands of samples. Moreover, the network is geared to bioagent identification and clinical diagnosis rather than microbial forensics.<sup>9</sup>

Another network being established at key sites and major cities throughout the country makes use of high-volume air collection and concentration stations. The filter paper samples taken from these various stations are then analyzed for the presence of bioagents at regular intervals of time, with the hope that a positive test could offer early warning that a bioattack has occurred. Such “detect to warn” and “detect to treat” capabilities help to complement the existing Laboratory Response Network and are an innovative part of our homeland security strategy.<sup>8</sup> Even large collections of such samplers, however, can monitor limited geographic areas only and, like the kinds of equipment mentioned next, are not intended for the comprehensive analyses of bioagents.

Portable and rapid testing equipment are also available, although they are limited for the detection of bioagents and do not adequately meet current biosecurity needs. The equipment produces positive/negative test results and works by amplifying and detecting a small number of genes that are always present in certain bioagents. Such technologies have several limitations: Each is designed to perform only one type of test, and each piece of equipment can process only a few dozen samples every few hours in the field. In addition, such technologies cannot produce the kinds of exact and complete data that are needed to differentiate one bioagent strain from another and cannot lead to the large volumes of data that are needed to track samples and attribute sources.<sup>10</sup>

The complete analysis of bioagents requires the types of laboratory procedures outlined below; each produces valuable information.

### Growing bioagents and testing their proteins and enzymes is needed for:

- determining susceptibility and resistance to drugs and vaccines
- seeking new ways to overcome resistance
- detecting signs of deliberate biological engineering

### Sequencing bioagent genes is needed for:

- tracking specific agents and isolates
- attributing specific agents and isolates to their sources
- detecting signs of deliberate biological engineering

### Archiving bioagent samples in long-term frozen storage is needed for:

- repeating tests at a later time
- performing new tests as they become available
- providing samples to other laboratories for independent analysis
- maintaining physical custody and evidence

The above laboratory procedures are repetitive, labor intensive, and well suited to high-throughput automation. At present, the largest users of such laboratory automation, precision robotics, and control technologies are biotech companies and large pharmaceutical firms. Their high-throughput screening and drug discovery laboratories can routinely perform a hundred thousand to a million tests per day. Such commercial technologies can also be incorporated into a high-throughput laboratory and information processing system against bioagents. In combination with the process control tools referred to above, commercial technologies provide the blueprint and building blocks for a biodefense sentinel.<sup>4,5</sup>

## MICROBIAL FORENSICS

Humans have unique genetic features, which makes it possible for DNA to be used as molecular fingerprints and evidence. However, the ultimate value of such information depends on the ability to compare an individual DNA sample against many others.<sup>10</sup> The same powerful approach also applies to bioagent forensics.

Bacteria such as *Bacillus anthracis* (anthrax) possess hundreds to thousands of sites, or hot spots, where their DNA exhibits variations.<sup>11,12</sup> The overall pattern and frequency of such variations can be used to differentiate one strain from another, distinguish one sample from another, and measure the relatedness of one sample to another. A

smaller number of variations between two samples is indicative of closer relations. Also, like human DNA, the analysis of more variable sites in anthrax DNA leads to more reliable fingerprints and evidence. At present, enough data exist to conclude that most if not all bioagents (bacteria and viruses) can be uniquely identified by genetic analyses, with one cautionary point to keep in mind. Certain bioagents have faster mutation rates than others and thereby exhibit a greater range of genetic variations, which makes them more amenable to tracing their origins. But even for bioagents with slowly mutating or monotonous genomes, the overall concept of distinguishing one sample from another still applies.

The next logical step is to build a comprehensive molecular fingerprint database of the most threatening bioagents and to use such information to track samples and attribute sources. Conceivably, such a database could grow to include 100,000 to 1 million samples analyzed over time. The only feasible way to achieve this goal is to build a high-throughput laboratory that takes advantage of automation, precision robotics, and control technologies. Such capabilities would eliminate the errors introduced by human technicians and make it feasible to perform every essential test on every sample. With this in mind, the utility of a high-throughput laboratory and database against bioagents is outlined below.

#### **The high-throughput laboratory and database is needed for:**

- saving lives and expediting recovery operations in response to attacks
- linking bioagent samples and sources efficiently
- testing all known variable sites in bioagents
- testing samples repeatedly for cell-to-cell or frequency-based signatures
- attributing bioagent sources through a combination of methods
- inferring bioagent histories through a combination of methods

In 1992, the Australia Group identified nearly 100 bacteria, viruses, fungi, and toxins against people, animals, and plants with potentials for weaponization. To date, however, fewer than 20 infectious agents have been used to produce biological weapons.<sup>13</sup> A realistic goal would therefore be to fingerprint and catalog this “low hanging fruit.” From a technical, economic, and political standpoint, the net result would be to increase the likelihood of attribution.<sup>14</sup>

### **DEMONSTRATION FACILITY**

A demonstration facility housing a flexible and computerized control system, automated and robotic sample

preparation and sequencing system, and information processing system could be built within a year. Following this engineering and integration phase, its capabilities could be demonstrated on a DNA-based bacterial pathogen and RNA-based viral pathogen over a second year. The effort would require a team of ten scientists and technicians and cost about \$7.5 million over two years, with \$4 million allocated for personnel, \$2 million for system equipment, and \$1.5 million for reagents and supplies.

The sequencing of DNA-based bacteria and RNA-based viruses by the same system would demonstrate its overall flexibility. *Bacillus anthracis* would be a logical choice because of its recognized potential for bioterrorism and because hundreds to thousands of sites within the anthrax genome are thought to exhibit natural and inherent variations.<sup>11,12</sup> Moreover, the frequency of these variations under various growth conditions and their associations to one another still require further detailed examination. Influenza virus would be another logical choice for several reasons.<sup>15</sup> Like many biothreat viruses, such as Ebola and Marburg hemorrhagic fevers, influenza viruses have RNA genomes that vary. Influenza is an infectious disease that profoundly affects human health and agriculture—a rapidly emerging pandemic could kill millions—and archives with thousands of samples are available for use.

The demonstration facility would be capable of fingerprinting all known variable sites in anthrax as well as sequencing all eight gene segments in influenza. The automated and robotic laboratory system would work with inactivated bioagent samples, thereby avoiding the need for a specialized containment space. This procedure would greatly speed work and reduce costs. In the event of an anthrax attack or influenza pandemic, however, the system could switch to working with active samples.

The computerized control system would allow secure access to the laboratory by way of the Internet, enable procedures to be designed in a flexible and programmable manner, schedule and perform numerous procedures on a routine basis, and deposit the results into a database. The control system’s design would be based on the design referred to above and take advantage of interface standards, which make it possible to use new technologies as they become available (see sidebar).

The automated and robotic sequencing system would be built on commercially available technologies. It would consist of modules that input samples and supplies, move them from place to place, prepare samples for sequencing, and sequence them by several different procedures. This architecture will increase sample throughput and also enable the system to serve as its own laboratory standard by generating comparable data different ways.

The information processing system would be built on commercially available database technologies. As shown in Figure 1, it would be capable of storing information with various levels of security.

### Attributes of a High-Throughput Laboratory

A high-throughput laboratory and database network could play a critical role in preventing, deterring, and responding to acts of bioterrorism. It could facilitate efforts taking place in public health, agricultural, emergency response, law enforcement, intelligence, and national security communities. Below is a summary of the attributes for such a network.

- High-throughput automated laboratories should be capable of performing 10,000 to 100,000 or more tests per day. Compared to manual laboratories, they should offer 100 to 1,000-fold improvements in sample processing speeds and volumes.
- High-throughput automated laboratories should be capable of operating 24 hours per day and 7 days per week. To do this, they must manage a continuous flow of supplies and samples and maintain quality controls on a daily basis.
- High-throughput laboratories should offer remote access and convenient means to submit samples from any geographic location. To do this, they must offer tools that work in conjunction with the Internet or secure intranets.
- High-throughput laboratories should support chain of custody procedures for law enforcement, homeland security, and national security efforts. For legally defensible and accurate attribution, the chain must be maintained from sampling integrity to data security.
- High-throughput laboratories should enable interconnectivity with other high-throughput laboratories. To do this, they should utilize a standard interface and operating system that leads to a national virtual capacity.
- High-throughput laboratories should adhere to a set of standards and specifications. The various ones relate to: labware, calibrations, communications, data structures, testing protocols, and data manipulation tools.
- High-throughput laboratories should be designed to incorporate technical improvements over time. Much like personal computers, they can be based on plug-and-play and modular architectures that facilitate upgrades in software and hardware.

### A FEW NETWORKED FACILITIES

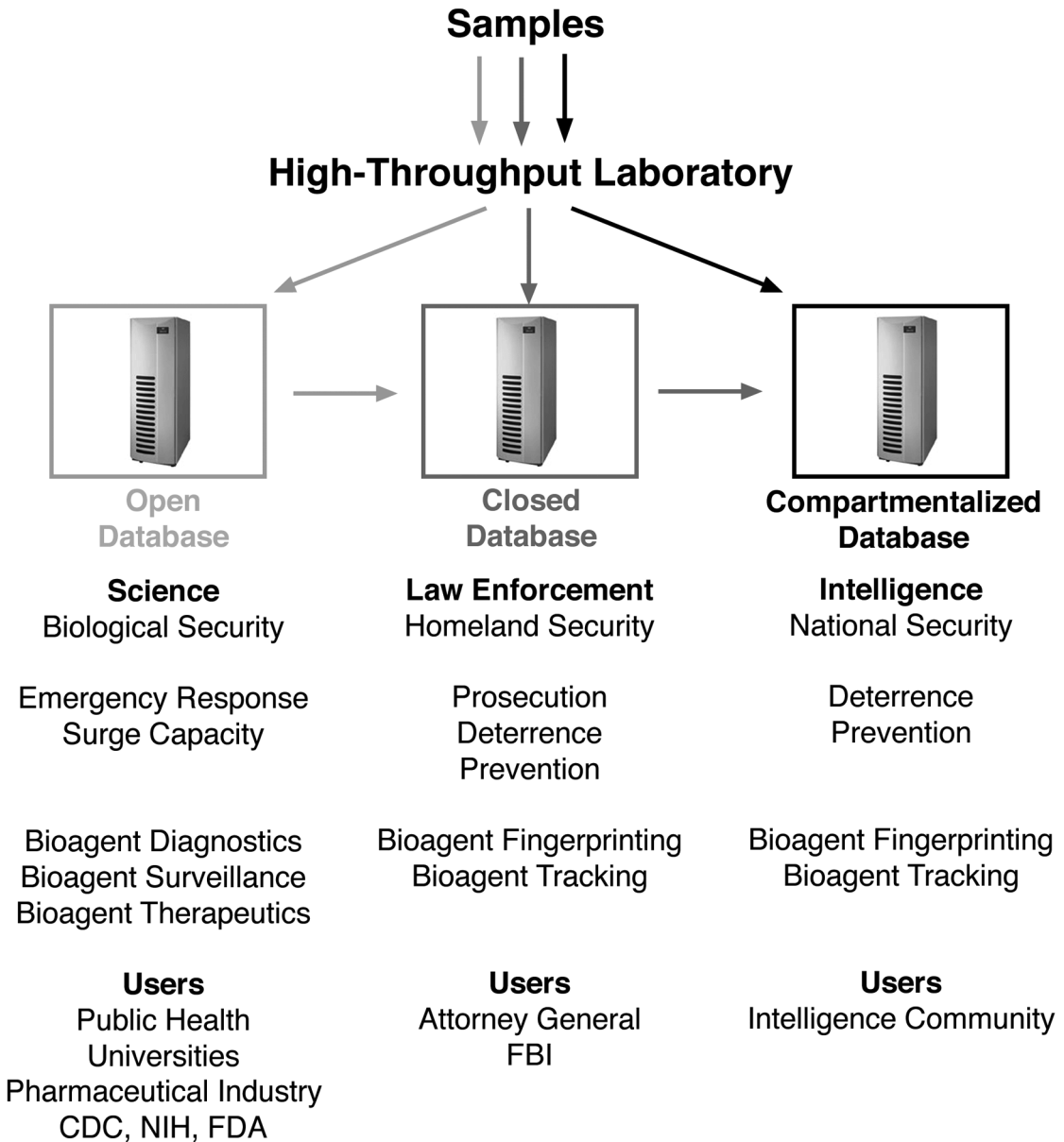
Successful operation of the above-described demonstration facility would enable the creation of a small but powerful network of high-throughput laboratories at key sites throughout the country. The location of these sites could relate to the bioagents they are approved to handle as well as other considerations mentioned below.

The CDC in Atlanta is the only institution in the country that can handle active variola virus (smallpox). As a result, a high-throughput laboratory at the CDC could play a vital public health role for a variety of reasons, but one stands out in particular. Smallpox was eradicated at the beginning of the molecular biology era, and, as a result, medical researchers have limited knowledge of variola's genetic variations and their role in transmissibility and virulence.<sup>16</sup> In 2001, a stunning scientific paper revealed that a bioengineered form of ectromelia virus or mousepox—a close relative of smallpox—was vaccine-resistant and more lethal in mice than the nonengineered form. The paper showed that inserting the interleukin-4 gene into mousepox was sufficient to confer these en-

hancements.<sup>17</sup> At present, it is unknown whether a similar interleukin-4 insertion in smallpox would confer vaccine resistance and greater lethality in humans, but these issues are a cause for real concern.

In the event of a smallpox outbreak, the nation's top public health advisors would want to rule out any possibilities of bioengineered virus and, consequently, would need to know the complete genetic makeup of the outbreak virus. To implement an optimal emergency response plan, they would need to have such detailed analyses overnight. A high-throughput laboratory operating at the CDC would offer the only realistic means to obtain such critical information.

After smallpox, the most threatening bioterrorist agents against people include *Bacillus anthracis* (anthrax), *Francisella tularensis* (tularemia), and *Yersinia pestis* (plague). The most threatening bioagents against food-producing animals include a short list of viruses, most notably foot-and-mouth disease virus. A strong argument could therefore be made to establish high-throughput laboratories at a small number of universities and government laboratories that currently conduct re-



**FIG. 1.** High-throughput laboratories would be capable of generating three categories of information: open, closed, and compartmentalized. The figure summarizes some of the potential applications and users of each category of information.

search and microbial forensics on the above weaponizable bioagents.

The National Research Council has recognized the need for accelerating research on microbial forensics and recommended the establishment of a national program on bioforensics analysis.<sup>8</sup> A network of five high-throughput laboratories and databases would help to fulfill these needs and recommendations at an estimated cost of \$75 million over 5 years. As outlined in the sidebar, the networked facilities would be built on the same principles and computerized control system as the demonstration one, leading to lower implementation costs and opera-

tional compatibility between sites. Instead of one automated and robotic laboratory system, however, various sites could house different kinds, including those that grow bioagents, test their proteins and enzymes, sequence variable sites and genes, and archive samples as outlined above.

**LONG-TERM VALUE**

New federal laws have been enacted that call for more safeguards, record keeping, and personnel checks at in-

stitutions that handle select bioagents.<sup>18</sup> In our quest to strengthen biosecurity, however, more time and money may be spent on adhering to new rules rather than on undertaking medical and scientific research. Clearly, we need to strike a balance between strengthening biosecurity and facilitating research on select bioagents. Here is where high-throughput laboratory and database systems could contribute: Forensic security can ease the burdens of physical security.

Some in the scientific community have begun to recognize that working with select bioagents is a privilege. In the future, researchers may be required periodically to submit samples of bioagents they are studying for high-throughput fingerprinting. The practice would automatically maintain a list of institutions and investigators who handle select bioagents and an up-to-date forensic database on them. If bioagents from a legitimate institution were ever used in a biological attack, we could uncover this quickly.

What about the rogue states, terrorist networks, and domestic terrorists who may have access to other sources of bioagents? In such cases, federal law enforcement and national security agencies have begun to assume a more proactive role. The shift in emphasis has required expanded efforts to monitor suspicious persons within our borders and expanded human intelligence operations abroad. As bioagent samples are collected through such means, the high-throughput laboratory would offer real-time microbial forensics for better biosecurity.<sup>19</sup>

Such combined efforts would enhance homeland and national security by:

- improving the means to prevent, deter, and react to bioattacks by rogue nations, terrorist networks, and domestic terrorists;
- producing databases that strengthen criminal investigations and prosecution efforts for the law enforcement community;
- providing rapid and complete information on bioattacks and thereby saving lives by expediting effective remedies and therapies;
- producing databases that are useful for developing new vaccines and drugs;
- effecting legally and politically defensible capabilities to collect, analyze, interpret, and preserve evidence against illicit biological programs and events; and
- helping to ensure the safety and readiness of troops stationed throughout the world.

The United States has plans for other complex and evolving threats. For example, it seeks to limit the proliferation of ballistic missile technology by gathering intelligence information, enacting export laws, and focusing diplomatic pressure. Nevertheless, if an enemy ever fired a missile at the United States, we would immediately pin-

point its origin with our “eyes in the sky” and act with guaranteed force. That is prevention, deterrence, and response rolled into one. The United States must now have the same sort of capability against bioterrorism. In terms of investment, every dollar spent on the high-throughput laboratory and database system will save much more.

## REFERENCES

1. Gellman B. 4 Nations thought to possess smallpox. *Washington Post* November 5, 2002;A1.
2. Layne SP, Sommer MH. A virus-fed doomsday. *Los Angeles Times* October 10, 2002;B21.
3. Layne SP. Virtually assured detection and response: Utilizing science, technology and policy against bioterrorism. In: Knobler SL, Mahmoud AAF, Pray LA, eds. *Biological Threats and Terrorism*. Washington, DC: National Academy Press; 2002:211–217.
4. Layne SP, Beugelsdijk TJ. Laboratory firepower for infectious disease research. *Nature Biotech* 1998;16:825–829.
5. Editorial. Beat bioterror with batch science. *Nature Biotech* 1998;16:793.
6. Layne SP, Beugelsdijk TJ. Method and apparatus for globally-accessible automated testing. 1988: U.S. Pat No 5,841,975.
7. Layne SP, Beugelsdijk TJ, Patel CKN. Tackling grand challenges with powerful technologies. In: Layne SP, Beugelsdijk TJ, Patel CKN, eds. *Firepower in the Lab: Automation in the Fight Against Infectious Diseases and Bioterrorism*. Washington, DC: Joseph Henry Press; 2001: 5–28.
8. National Research Council. Human and agricultural health systems. In: *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, DC: National Academy Press; 2002:65–106.
9. Gilchrist MJR. The progress, priorities, and concerns of public health laboratories. In: Knobler SL, Mahmoud AAF, Pray LA, eds. *Biological Threats and Terrorism*. Washington, DC: National Academy Press; 2002:160–165.
10. Murch RS. Forensic perspective on bioterrorism and the proliferation of bioweapons. In: Layne SP, Beugelsdijk TJ, Patel CKN, eds. *Firepower in the Lab: Automation in the Fight Against Infectious Diseases and Bioterrorism*. Washington, DC: Joseph Henry Press; 2001:203–213.
11. Keim P, Price LB, Klevyiska AM, Smith KL, Schupp JM, Okinaka R, Jackson PJ, Hugh-Jones ME. Multiple-locus variable-number tandem repeat analysis reveals genetic relationships within *Bacillus anthracis*. *J Bacteriol* 2000;182:2928–2936.
12. Read TM, Salzberg SL, Pop M, Shumway M, Umayam L, Jiang L, Holtzapple E, Busch JD, Smith KL, Schupp JM, Solomon D, Keim P, Fraser CM. Comparative genome sequencing for discovery of novel polymorphisms in *Bacillus anthracis*. *Science* 2002;296:2028–2033.
13. Christopher GW, Cieslak TJ, Pavlin JA, Eitzen EM. Biological warfare: A historical perspective. *J Am Med Assoc* 1997;278:412–417.
14. Fraser CM, Dando MR. Genomics and future of biological

- weapons: The need for preventive action by the biomedical community. *Nature Genetics* 2001;29:253–256.
15. Layne SP, Beugelsdijk TJ, Patel CKN, Taubenberger JK, Cox NC, Gust ID, Hay AJ, Tashiro M, Lavanchy D. A global lab against influenza. *Science* 2001;293:1729.
16. LeDuc JW, Damon I, Meegan JM, Relman DA, Huggins J, Jahrling PB. Smallpox research activities: U.S. interagency collaboration, 2001. *Emerg Inf Dis* 2002;8:743–745.
17. Jackson RJ, Ramsay AJ, Christensen CD, Beaton S, Hall DF, Ramshaw IA. Expression of mouse interleukin-4 by a recombinant Ectromelia virus suppresses cytolytic lymphocyte responses and overcomes genetic resistance to mousepox. *J Virol* 2001;75:1205–1210.
18. U.S. Congress. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. October 25, 2001.
19. Layne SP, Fraser CM. Scientific speed is the key in fighting bioterror. *Los Angeles Times* May 1, 2002;B13.

Address reprint requests to:

Scott P. Layne, MD

School of Public Health

University of California, Los Angeles

P.O. Box 951772

Los Angeles, CA 90095-1772

E-mail: spl@lvik.ph.ucla.edu

Published online: May 2, 2003