

The Role of High-Throughput Laboratories in Homeland Security

Tony J. Beugelsdijk^{1,*} and Scott P. Layne²
¹Los Alamos National Laboratory; ²School of Public Health,
 University of California, Los Angeles

Keywords:

high-throughput testing, automation, infectious disease, SARS, influenza, anthrax, smallpox, biological weapons, homeland security, epidemiology, surveillance

Infectious diseases pose threats from natural and manmade sources, and arguably the situation is getting worse. The outbreak of the coronavirus causing the severe acute respiratory syndrome (SARS) shows that the world is linked by thousands of people traveling millions of miles every single day who can spread SARS or new strains of influenza with pandemic potential.¹ The world is also becoming a more dangerous place, with rogue nations and terrorist networks aggressively seeking nuclear, chemical, and biological weapons. Of these, biological weapons are the cheapest to produce and likely the most attractive because they can be used anonymously (JALA 2003;8:11–18)

INTRODUCTION

To this day, we do not know whether the perpetrator of the post-9/11 anthrax letter attack was an organized “bio bin Laden” or a lone “bio Kaczynski.” Because of extensive media coverage, however, we do know that the leaders of rogue nations and terrorists networks see biological attacks in more threatening ways. 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 (see Table 1).

The above remarks point to two inescapable problems. Both natural and manmade infectious disease outbreaks pose significant threats to our homeland security. Such outbreaks can create emergency situations that require enormous quantities of accurate information to help guide life-saving actions. How can these problems be addressed?

This article describes a new role for high-throughput automated laboratories in the fight against infectious diseases. More specifically, it emphasizes how available laboratory technologies can be coupled with strategic plans to prevent, deter, and respond to bioterrorist attacks. It is also clear, however, that many of the same technologies and concepts can be applied to the control of natural infectious disease outbreaks (Figure 1).

A NEW VISION FOR BIOLOGICAL DEFENSE

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

*Correspondence: Tony J. Beugelsdijk, Ph.D., M.B.A., IBD Division, MS C333, Los Alamos National Laboratory, P.O. Box 1663, Los Alamos, NM 87545; Phone: +1.505.667.3169; Fax: +1.505.665.3125; E-mail: beugelsdijk@lanl.gov

Copyright © 2003 by The Association of Laboratory Automation

1535-5535/2003/\$30.00 + 0

doi:10.1016/S1535-5535(03)00004-2

Table I. Comparison of nuclear and biological threats

	Nuclear	Biological
Material	Under tight control, few sources	Not controlled, ubiquitous sources
Practitioners	Small community	Very large community
Know-how	Classified	Open literature
Primary driver	Public sector—defense, energy	Private sector—financial, health care
Barriers to entry	Very high, regulated	Extremely low, minimal self-regulation
Technology footprint	Very large, detectable	Very small, undetectable
Impact	Immediate, large, but localized	Delayed, large, can get much larger
Fingerprint	Isotopic composition	Sequence databases
Prevention	Nonproliferation treaties, inspections	Improbable
Deterrence	MAD	Rapid attribution

crisis, it would offer much needed surge capacity to the network of public health laboratories operating throughout the country. Such front-line 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 counter-terrorism and non-proliferation that can be

summed up as: virtually *assured detection, attribution, and response (VADAR)*.²

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 1998.³ An editorial in the same journal called attention to the plan's importance and called for action.⁴ 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.⁵ Alto-



Figure I. The operation of high-throughput laboratories and databases would follow the same organization and logistics for natural and manmade infectious disease threats.

gether, 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 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.⁶ Before 9/11, these foundations helped to shape scientific thinking, but afterwards they galvanized a broader consensus.

In 2002, the National Academies published a 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.⁷

CAPABILITIES, TESTS, AND APPLICATIONS

The Centers for Disease Control and Prevention 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.⁸

During the 2001 anthrax letter attacks, the Laboratory Response Network was called upon 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.⁸

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.⁷ 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 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.⁹

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 are 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 bio-defense sentinel.^{3,4}

MICROBIAL FORENSICS

Humans have unique genetic features, which make 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.⁹ 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.^{10,11} 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. The 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 exists 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.¹² A realistic goal, therefore, would 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.¹³

HIGH-THROUGHPUT LABORATORY ATTRIBUTES

All of the necessary hardware components exist to build true high-throughput automated laboratories and databases to prevent, deter, and respond to bioterrorist acts. In the coming years, such systems could facilitate efforts taking place in public health, agricultural, emergency response, law enforcement, intelligence, and national security communities.⁶ Building and maintaining credible systems for biological defense, however, will take more than simply purchasing all the individual hardware components from manufacturers that can perform the kinds of laboratory procedures summarized above. A larger set of issues must be taken into account.⁷ Below are seven key attributes that can be used to define true high-throughput systems.

1. Processing capacity. High-throughput laboratories should offer significant increases in the number of tests performed and/or samples processed per day compared to purely manual laboratories. For various tests and protocols, they should offer at least 100- to 1,000-fold improvements over manual laboratories. Many laboratory automation and robotic manufacturers offer components that can support such increases in throughput but, as described below, the right kinds of supporting infrastructures are also needed.
2. Sustainability of operation. Many high-throughput laboratories that are currently in use cannot sustain 24/7 operation. Several reasons account for this situation. Equipment manufacturers and system integrators often estimate operational capacity based on the automated and robotic system itself. But such estimates often overlook the overall flows and loads within laboratories that reduce throughput, including the management of proper supply chains and having formal validation procedures and quality controls in place. In addition, even though current automated and robotic systems are robust, they still exhibit recoverable faults that require minimal intervention and occasional non-recoverable failures that require downtime for maintenance. Because true high-throughput laboratories must sustain 24/7 operation, their overall evaluation needs to include a proper reliability, availability, and maintainability (RAM) statistical analysis to understand their realizable (not designed) sustainability of operation.¹⁴ Standard reliability engineering studies would also develop loss trees that discover where reductions from designed capacities occur. These can take the form of availability, operability, maintainability, risk management, and quality losses.

3. Adherence to standards. Because high-throughput laboratories can generate enormous quantities of data very fast, they can also generate enormous quantities of flawed data very fast. Consequently, nothing is gained by performing non-reproducible or non-validated assays in high-throughput modes. The key to generating reproducible and robust data is adherence to a variety of standards. These range from instrument-based standards that include labware, control diagnostics, measurement calibrations, communications and data formats, and data manipulation tool sets to assay-based standards that include standardized reagents, cell lines, and protocols. In the past, efforts have been made to develop both types of standards, but more needs to be done because high-throughput data is widely regarded as “noisy.” The sources and magnitudes of the various components to this noise remain unclear in large part because adherence to standards has been overlooked.
4. Chain of custody. In order to attribute a bioagent to a particular source, the high-throughput laboratory must adhere to established procedures for handling, testing, and maintaining legal evidence. Such procedures must begin before samples arrive at the laboratory and include appropriate training of collectors and maintaining chain of custody records for samples.⁹ The raw data generated by the high-throughput laboratory must also be secured, backed up, and deemed tamper proof.
5. Interconnectivity with other high-throughput laboratories. Homeland security demands that each and every high-throughput laboratory utilize the same operating system that enables interconnectivity and interoperability to create a virtual national capacity. Such a network of systems will enable an on-demand, high-throughput capacity that can scale and be utilized in the event of a national emergency. Inherent to this capability is a uniform set of operating system standards for all high-throughput laboratories. Various representations of capability datasets need to be implemented from the device level to the national level in the hierarchy shown below.

National
Enterprise
Laboratory
System
Device

At the lowest or device level, for example, the Device Capability Dataset (DCD) describes idiosyncratic characteristics as the equipment’s identity, physical dimensions, location, supported command set, generated events, input-output (I/O) ports, and other resources. The capability dataset concept provides a means for standardizing the interface of laboratory automation devices and integrating them into self-describing systems, laboratories, enterprises, and national capacities in a descriptive rather than a prescriptive manner. The capability dataset is a key concept for building standardized and

remotely accessible systems with flexible architectures. Without it, more cumbersome “wrapper” codes are needed to map various manufacturer’s components and systems onto a set of standard representations.

6. Remote accessibility. To quickly configure a network of high-throughput laboratories into a virtual capability, the individuals systems need to be remotely accessible. A series of web-enabled process control tools have been described that facilitate programming of tests, operation of laboratory equipment, and analysis of data. These software tools work in conjunction with a scheduler and task sequence controller.
7. Flexibility to adopt new technology. A modular architecture and foundation for the design of high-throughput laboratories offers a relatively easy path for upgrading components. As a newer and more efficient hardware component becomes available, for example a more advanced microcapillary array sequencer, it can replace an older one having less resolution and sequencing capacity. In this instance, the code for the testing procedure remains the same as do the data analysis routines. In older non-modular systems, such replacements would involve tedious reprogramming and thereby prevent innovations and upgrades.

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 10 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 fingerprinting of DNA-based bacteria and RNA-based viruses by the same system would demonstrate its overall flexibility. *Bacillus anthracis* (anthrax) 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.^{10,11} 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.¹⁵ Like many biothreat viruses, such as Ebola and Marburg hemorrhagic fevers as well as SARS, influenza viruses have RNA genomes that vary. Influenza is an infectious disease that profoundly impacts 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.

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 2, it would be capable of storing information with various levels of security.

NETWORKED AND VIRTUAL FACILITIES

Successful operation of the above 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 Centers for Disease Control and Prevention (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.¹⁶ 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 non-engineered form. The paper showed that inserting the interleukin-4 gene into mousepox was sufficient to confer these enhancements.¹⁷ At present, it is unknown whether a similar interleukin-4 insertion in smallpox would confer vaccine resistance and greater lethality in humans, and these issues are a cause for real concern.

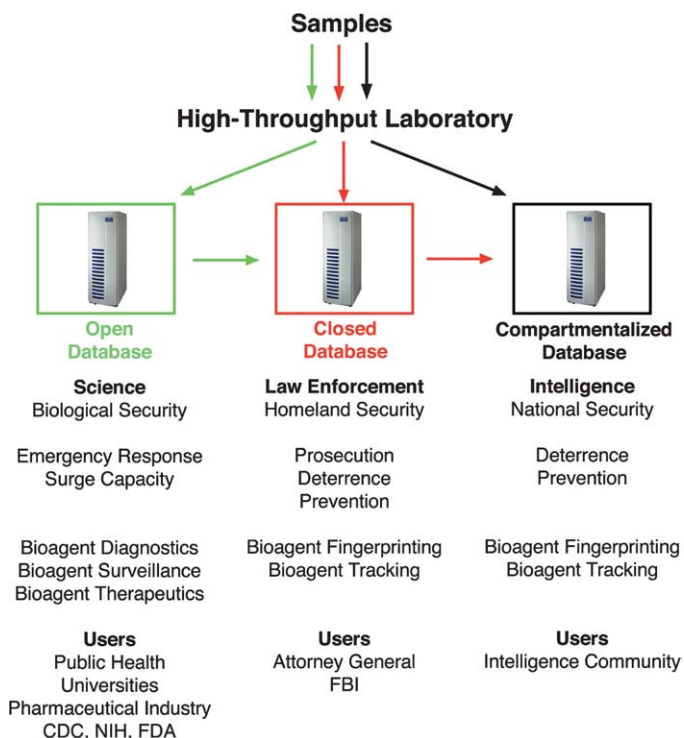


Figure 2. High-throughput laboratories would be capable of generating three categories of information: open, closed, and compartmentalized. The figure summarizes some of the potential applications and users of each category of information.

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 research 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.⁷ 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 five years. The networked facilities would be built on the same principles and computerized control system as the demonstration one, leading to lower implementation costs

and operational 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.

OVERALL VALUE

New federal laws have been enacted that call for more safeguards, record keeping, and personnel checks at institutions that handle select bioagents.¹⁸ 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.¹⁹

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 pinpoint 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. Layne, S. P. Put high-tech labs into the fight against SARS and Bioterrorism. *Los Angeles Times*, April 4, 2003, pp B17.
2. Layne, S. P. Virtually assured detection and response: utilizing science, technology and policy against bioterrorism. In *Biological Threats and Terrorism*; Knobler, S. L., Mahmoud, A. A. F., Pray, L. A., Eds.; National Academy Press: Washington, DC, 2002; pp 211–217.
3. Layne, S. P.; Beugelsdijk, T. J. Laboratory firepower for infectious disease research. *Nat. Biotechnol.* **1998**, *16*, 825–829.
4. Editorial. Beat Bioterror with Batch Science. *Nat. Biotechnol.* **1998**, *16*, 793.
5. Layne, S. P.; Beugelsdijk, T. J. Method and apparatus for globally-accessible automated testing. U.S. Patent 5,841,975, 1988.
6. Layne, S. P.; Beugelsdijk, T. J.; Patel, C. K. N. Tackling grand challenges with powerful technologies. In *Firepower in the Lab: Automation in the Fight Against Infectious Diseases and Bioterrorism*; Layne, S. P., Beugelsdijk, T. J., Patel, C. K. N., Eds.; Joseph Henry Press: Washington, DC, 2001; pp 5–28.
7. National Research Council. Human and agricultural health systems. In *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*; National Academy Press: Washington, DC, 2002; pp 65–106.
8. Gilchrist, M. J. R. The progress, priorities, and concerns of public health laboratories. In *Biological Threats and Terrorism*; Knobler, S. L., Mahmoud, A. A. F., Pray, L. A., Eds.; National Academy Press: Washington, DC, 2002; pp 160–165.
9. Murch, R. S. Forensic Perspective on Bioterrorism and the Proliferation of bioweapons. In *Firepower in the Lab: Automation in the Fight Against Infectious Diseases and Bioterrorism*; Layne, S. P., Beugelsdijk, T. J., Patel, C. K. N., Eds.; Joseph Henry Press: Washington, DC, 2001; pp 203–213.
10. Keim, P.; Price, L. B.; Klevyiska, A. M.; Smith, K. L.; Schupp, J. M.; Okinaka, R.; Jackson, P. J.; Hugh-Jones, M. E. Multiple-locus variable-number tandem repeat analysis reveals genetic relationships within *Bacillus anthracis*. *J. Bacteriol.* **2000**, *182*, 2928–2936.
11. Read, T. M.; Salzberg, S. L.; Pop, M.; Shumway, M.; Umayam, L.; Jiang, L.; Holtzapple, E.; Busch, J. D.; Smith, K. L.; Schupp, J. M.; Solomon, D.; Keim, P.; Fraser, C. M. Comparative Genome Sequencing for Discovery of Novel Polymorphisms in *Bacillus anthracis*. *Science* **2002**, *296*, 2028–2033.

12. Christopher, G. W.; Cieslak, T. J.; Pavlin, J. A.; Eitzen, E. M. Biological warfare: A historical perspective. *J Am. Med. Assoc.* **1997**, *278*, 412–417.
13. Fraser, C. M.; Dando, M. R. Genomics and future of biological weapons: the need for preventive action by the biomedical community. *Nat. Genet.* **2001**, *29*, 253–256.
14. Grundmann, J. G. Reliability, availability and maintainability for a laboratory automated storage and retrieval system. *Laboratory Robotics and Automation* **1989**, *1*, 95–104.
15. Layne, S. P.; Beugelsdijk, T. J.; Patel, C. K. N.; Taubenberger, J. K.; Cox, N. C.; Gust, I. D.; Hay, A. J.; Tashiro, M.; Lavanchy, D. A global lab against influenza. *Science* **2001**, *293*, 1729.
16. LeDuc, J. W.; Damon, I.; Meegan, J. M.; Relman, D. A.; Huggins, J.; Jahrling, P. B. Smallpox research activities: U.S. Interagency collaboration 2001. *Emerging Inf. Dis.* **2002**, *8*, 743–745.
17. Jackson, R. J.; Ramsay, A. J.; Christensen, C. D.; Beaton, S.; Hall, D. F.; Ramshaw, I. A. 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, S. P.; Fraser, C. M. Scientific speed is the key in fighting bioterror. *Los Angeles Times*, May 1, 2002, p. B13.