Meeting the Chem–Bio Defense Challenge

Darryl Greenwood

Biological and chemical agents are a significant and growing risk to society. Traditionally thought of as agents of war, these materials are likely to be used by terrorists of the future. This threat is well recognized at the national level; the Department of Defense, Department of Homeland Security, and various government agencies are making significant investments in chemical and biological defense. At Lincoln Laboratory, research on chemical and biological defensive measures began in 1995 and has since grown into a formal Laboratory mission area. Principal activities are in sensor development and testing, facility defense, integrated systems, decision support, and medical surveillance. Many of the Laboratory's prototypes have found their way into operational systems through effective technology transfer.

Biological and chemical agents in the wrong hands can be used to cause great harm to people and cause great disruption to society. Aum Shinrikyo's release of nerve gas in the Tokyo subway system and in Matsumoto demonstrated the potential for and the will of terrorists to injure civilians with chemical warfare agents. The unknown person who mailed anthrax to news media and to the Congress inflicted just a few casualties but caused substantial disruption and cost to the U.S. government. Knowledge of foreign programs (e.g., through the efforts of the UN following Operation Desert Storm) has opened the eyes of national leaders to the potential threats in the hands of people intent on damaging American society.*

Thankfully, no chemical attack has caused major loss of life since World War I, and no biological attack has been successful at a large scale. Because of treaties and a general repugnance to the use of such agents, nation-states are very wary about being seen developing or using chemical or biological weapons for fear of being ostracized or worse. Because chemical and biological materials are dangerous to work with and not widely available, it takes considerable technical skill (as well as a bit of luck) to build, deploy, and use such weapons. Still, published accounts make clear that terrorist organizations and individuals seek these weapons and, having them, could use them to maximum effect.

Lincoln Laboratory began working on countermeasures to biological and chemical weapons in the mid-

* This article is based on a variety of reference material, all generally considered common knowledge. Thus the author has chosen to provide a brief bibliography at the end rather than a detailed list of individual citations.

FIGURE 1. Copies of the 2001 letters containing anthrax that were mailed to senators and news media (*New York Times,* Jan. 6, 2002). The perpetrator has never been identified, and now six years later, the FBI maintains a large task force dedicated to solving this crime.

1990s. We believed that existing defense measures could benefit from a fresh look with new approaches. We saw this as a critical national-security problem, with technology offering the potential to minimize or even totally negate the effects of these weapons.

National Efforts

Throughout the 1970s and 1980s, U.S. biological and chemical defense research was not a high priority for the Department of Defense. During that period, the National Institutes of Health and the Centers for Disease Control and Prevention (CDC) pursued biological defenses solely in the context of infectious disease and public health. A few events changed the national perspective, bringing a sense of urgency. With the end of the Cold War, the U.S. government discovered the breadth and depth of the former Soviet Union's offensive chemical and biological warfare program. Likewise, following the U.S. invasion into Iraq in 1991, the United Nations and the West were able to obtain supporting evidence of Iraq's significant offensive biological warfare program. In 1995, the world saw the release of the nerve gas sarin in Tokyo subways. Taken together, these events influenced the U.S. government to invest more heavily in research on chemical and biological defense. The realization that U.S. forces might have faced a significant chemical or biological threat in the 1991 Gulf War heightened worries—and therefore the chem–bio defense budget—in the 1990s.

The event that gave chemical and biological defense research even higher priority was the October 2001 dissemination of the anthrax-causing agent via postal envelopes (Figure 1). This attack, coupled with generalized intensification of concern after September 11 about terrorists' sophistication and capabilities, led to heightened urgency about this research. The Department of Defense saw modest budget increases, and major programs were started in the new Department of Homeland Security (DHS) and within the Department of Health and Human Services (DHHS). Most notably, DHHS investment in biodefense shot up in one year to more than $1 billion, and within a few years approached $4 billion (Figure 2). The work supported by these increases was medical in nature, as distinct from the development of new technology, which was left to the Defense and Homeland Security departments. Much of the funding surge went not just to research but to improving infrastructure and to stockpiling drugs.

A measure of the federal response is funding and reorganization, and both have happened. To assess the success of this effort in biological and chemical defense, we need to ask how much capability we now have as a nation to stop or minimize a biological or chemical attack. That is difficult to measure in the absence of any real trial,

such as a major attack. Additionally, because biological and chemical weapons are difficult to detect prior to use (i.e., when they are in development and production), most of the federal spending on chem–bio defense goes to support a detect-to-treat doctrine. Inherent in the current approach is an effort to identify a specific medical treatment for each threat agent—that is, one bug, one drug.

Absent an attack on the United States or some other cataclysmic event, the current approach will probably prevail for some time. Clearly, however, much more capability is needed. Some urge a focus on a broad-spectrum prophylaxis or treatment—but despite decades of effort no such elixir has appeared. Even the antibiotics of the 20th century have lost potency because of constant pathogen mutation. On another front, technology in the form of collectors and sensors offers the potential for quicker and more reliable alarms that harmful agents have been released—a sensible approach, given that many of the diseases are treatable if diagnosed in time. A third approach is to concentrate on rapid medical diagnosis. Because of the difficulty and importance of the problem, all reasonable avenues should be pursued.

A future administration may have different priorities for defending against chemical and biological weapons. Those working this problem should therefore be looking for ways to make their achievements fulfill a dual use—not only to bolster defense against an attack but also to help deal with phenomena unrelated to war or terrorism, such as disease, hazardous materials, and catastrophic natural events. After all, the urgency of biodefense may fade over time, but public health is a constant top priority. Ideally, barriers between civil and military capabilities dealing with such disasters (including a biological release) will have to be lowered.

Lincoln Laboratory Program

Chemical and biological defense presents a challenge consistent with the mission of Lincoln Laboratory. Here is a threat to national security that could be addressed, at least in part, by an investment in technology. In 1995 the Laboratory, having worked for decades on ballistic missile defense, satellite communications, and space surveillance, was looking to make new contributions to national security. Over the following years, several technical efforts

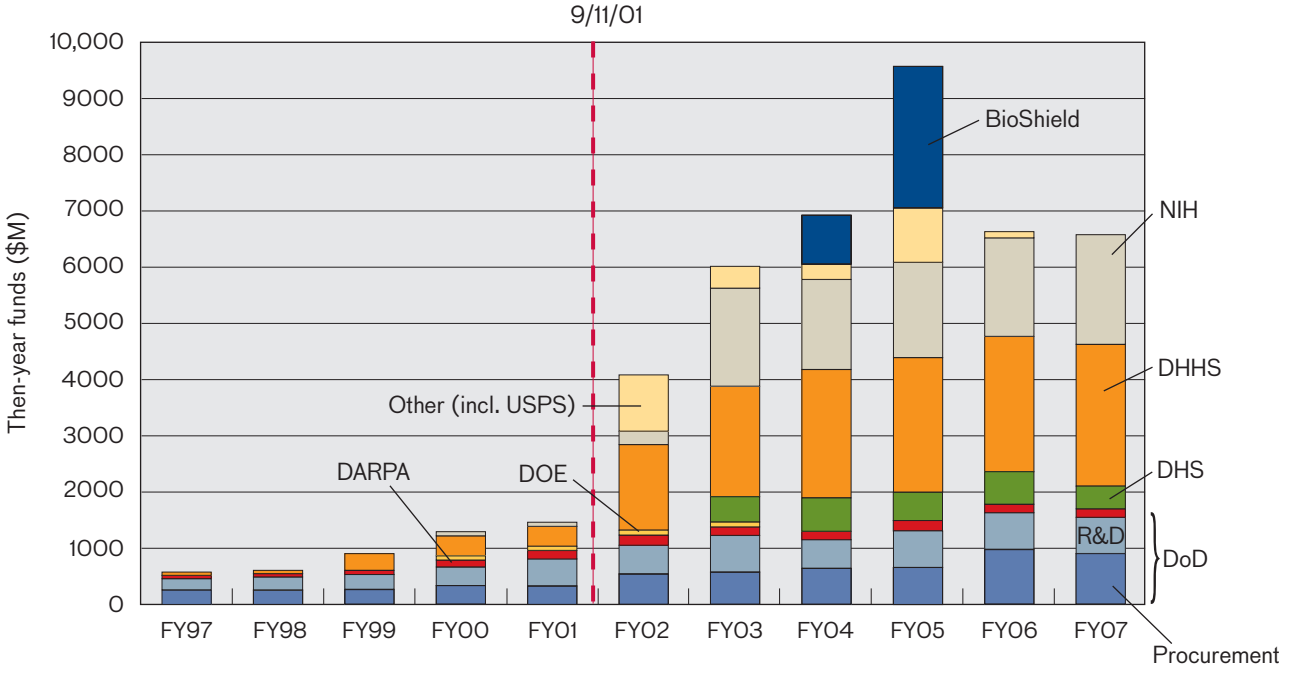

FIGURE 2. Total federal funding for biological and chemical defense has surged in recent years. The Department of Health and Human Services (DHHS) budget—including the Centers for Disease Control—is shown separate from that of the National Institutes of Health (NIH), to reflect the distinct emphasis of NIH on medical research. The Department of Defense has largely stayed the course, with modest increases through this period. The Defense Advanced Research Projects Agency (DARPA) appears prescient, having started its program in the early 1990s and maintaining a greater than $150 million effort for many years. Although chemical and biological funds are lumped together, biodefense work accounts for about 90% of the total.

stand out and are reviewed in this issue of the *Journal*. The holy grail of biological and chemical sensing is to do it at distance, so that there is time to react and invoke protective measures. In 1995, Lincoln conducted a brief study for the Joint Program Office for Chem–Bio Defense on a biological agent standoff approach that uses a laser radar (lidar) operating in the ultraviolet. The Laboratory reported how the physics of the atmosphere limited the performance of such systems. Backgrounds and the atmosphere invariably limit standoff performance—a theme that will repeat itself. Because of these basic limitations, the Laboratory has been exploring different sensors and sensing architectures. The report by Juliette Seeley and Jonathan Richardson (page 85) describes a low-cost architecture for early warning sensing, as well as a new design for a staring standoff sensor.

In 1996, the Army's Edgewood Chemical Biological Center funded a seedling technology effort to develop a biological agent warning sensor, or BAWS. The technology was based on the knowledge that almost all organisms contain the amino acid tryptophan, which fluoresces under ultraviolet light. Because tryptophan fluorescence is non-specific, BAWS alone cannot identify a pathogen; rather, it serves as a trigger to bring into action a subsequent analyzer or identifier. From receipt of funding in February 1996 to scored field trials at the Army's Dugway Proving Ground took just seven months, a tribute to the ability to rapidly prototype a concept to see if it would work in practice. In 2000, the Laboratory transitioned its BAWS work to industry production. BAWS is now entering its fifth generation. The article by Thomas Jeys and colleagues (page 29) describes work on advanced trigger technologies, which improve on BAWS cost and performance.

Once a sensor triggers that a bio-agent may be present, a sample of the suspect material needs to be collected and analyzed. There are a number of approaches to bio-identification, the most prominent of which are polymerase chain reaction (PCR) and immunoassay (such as that used in a physician's strep test kit). A Lincoln Laboratory variant on the immunoassay is an identifier based on a type of white blood cell, or B cell, where murine B cells are made to interact with the unknown analyte. The B cells are genetically modified to recognize specific analytes and within seconds signal binding to the analyte by emitting light. In 1998, the Defense Advanced Research Projects Agency (DARPA) funded a collaboration between Lincoln Laboratory and the MIT Cancer Center to develop the B-cell approach in a project called CANARY (cellular analysis and notification of antigen risks and yields). The article by Martha Petrovick, Mark Hollis, James Harper, and colleagues (page 63) shows the promise of this approach, which has been fielded in a number of locations.

Although PCR's extremely good specificity and sensitivity makes it the identifier of choice, the technique has one major shortcoming: it can be slow if there is a need to prepare samples. Lincoln Laboratory therefore chose to emphasize sample preparation in its technology program, and specifically dealt with dirty samples such as would be collected from the environment. Lalitha Parameswaran and colleagues report on their sample preparation work on page 167.

Biological and chemical weapons are difficult to detect prior to their use—that is, when they are in development and production.

Taking a System Approach

The first five or so years of this program area at the Laboratory emphasized technology push. That is, staff members had bright ideas for technology that might be useful for certain applications. Following the attacks of 2001, however, a cottage industry that sprang up across the country promised all kinds of technologies to detect and identify biological and chemical agents. Given this proliferation, the Laboratory chose to make a strategic shift to the applications, or system, side of the equation.

This change required a shift in mindset. First, activities would be requirements-driven in an analytical process based on perceived threats and vulnerabilities. Second, system architectures would be postulated based on a requirements process. These architectures require components, but they also require a well-defined concept of operations. If the architecture can be effected with existing components, then one should go ahead to develop and deploy such a system. If there are shortfalls in existing

The Threat

A short guide to the chemical and biological agents that must be defended against.

Chemical warfare agents are classified in three main groups:

- Blister or vesicant agents (i.e., mustard, lewisite, and phosgene oxime) burn and blister the skin or any other membrane they come in contact with. These are the chemicals used in Europe during World War I and against the Kurds by Saddam Hussein in the 1980s. Their persistence can be increased by dissolving them in nonvolatile solvents, thus making them difficult to remove from various materials. Many of these agents have legitimate industrial uses.
- Choking agents (e.g., phosgene, diphosgene, chlorine, and chloropicrin) attack lung tissue, predominantly causing pulmonary edema. Some of these agents have legitimate industrial purposes as well.
- Nerve agents (e.g., tabun, sarin, soman, cyclosarin, and VX) inhibit the action of the enzyme acetylcholinesterase, causing sustained muscular spasms that can lead to asphyxiation. None of these agents have legitimate purposes, given their toxicity, though related chemicals have been used as pesticides.

All of these materials are governed by the Chemical Weapons Convention and other treaties limiting production, stockpiling, and use as chemical warfare agents.

Until the 1990s, the chemical threat stopped there. Now, however, there is great concern over the potential for terrorists obtaining and using toxic industrial chemicals. These agents, including such chemicals as formaldehyde, ammonia, and chlorine, are readily available within the United States, as they are produced in quantity, stockpiled, and transported across the country in tanker trucks and rail cars. These chemicals are less toxic than chemical warfare agents, and first responders have experience dealing with them. Nonetheless, their intentional release could cause significant disruption and loss of life.

The biological threat is not as well understood as the chemical one. The most familiar biological agent—anthrax—has been around a long time as an infectious killer of animals. It is a bacillus that forms spores, thus making it very hardy in the environment. Inhalational anthrax has been an occupational hazard ever since humans began working animal hides. It is generally fatal once symptoms appear, but can be treated pre-symptomatically with antibiotics, and there is an effective vaccine. The United States, the Soviet Union, Britain, and other nations developed anthrax weapons in the 1940s through the 1960s. Because of its stability, availability, and infectiousness, anthrax is considered the top biological warfare threat.

Other bacteria and viruses are likewise of concern if they are sufficiently stable, are infectious, and cause fatal or debilitating disease. The Centers for Disease Control and Prevention (CDC) publishes a list of these agents of concern (www.bt.cdc.gov/agent/agentlist-category.asp). In reviewing these agents, a few points must be kept in mind. First, all bacterial illnesses are treatable with antibiotics. Yes, some strains are antibiotic resistant, but in principle diseases caused by bacteria can be brought under control with drug treatment, provided the treatment is timely and correct to the agent. The issue, then, is not whether treatment is possible, but whether in the event of a major bio-attack the treatments could be brought to the individuals fast enough.

For viral bio-agents such as smallpox, Ebola, SARS, or pandemic flu, the situation is much

capabilities, then new technology must be developed or even invented. This process is illustrated in Figure 3.

As an R&D organization, Lincoln Laboratory naturally spends a great deal of time on technology development and experimentation—i.e., in the upper right part of this process diagram. But as a technology-solutions house, the Laboratory works over the entire field, incorporating off-the-shelf components and conducting lab and field

more complex. There are few vaccines—only some of which are used routinely—and even fewer anti-viral medicines. Generally, we depend on our body's immune system to fight off viral infections. A notable exception is smallpox, in that the same vaccine that provides immunity to the disease also works as a treatment (if administered quickly enough).

Biological agents are a more challenging threat than chemical ones, not least because lethal quantities are smaller by orders of magnitude. Moreover, biology is changing daily, and it is inherently dual-use. DNA sequences of many bio-agents have been published. In the not too distant future, biologists will be able to e-mail a sequence to a microbe foundry and produce from scratch a designer bio-agent. Already there have been publications about synthesized polio and about resequencing the long-gone (and catastrophically deadly) 1918 flu virus. All this is done in the interest of science and with a desire to develop countermeasures to what could be the next pandemic.

Further, understanding the genome allows for genetic manipulation. Researchers have published papers describing the insertion of toxin-producing genes into otherwise harmless microbes. These techniques are used for legitimate purposes in agriculture and in pesticides. Sometimes, as happened with the mousepox gene manipulation in Australia, an unexpected consequence occurs [1]. Scientists researching mouse birth control inadvertently knocked out the mouse's immune system. They transformed a disease that their mice were immune to into one that killed the mice no matter their defenses. This surprising result suggests that it may be easier than we thought to transform a virus from a benign to a lethal one.

Gene manipulation is of course nothing new. It has been going on in nature since the beginning of the first life forms. Microbes—even those of different genus and species from one another—are constantly exchanging DNA, determining by trial and error if the new additions are favorable. Even the development of antibiotic resistance in bacteria was first established without knowledge of genes or DNA. Perhaps the specter of genetic manipulation is not as dire as some would want us to believe. After all, nature has been at this for a very long time. It might be hard to improve on her product.

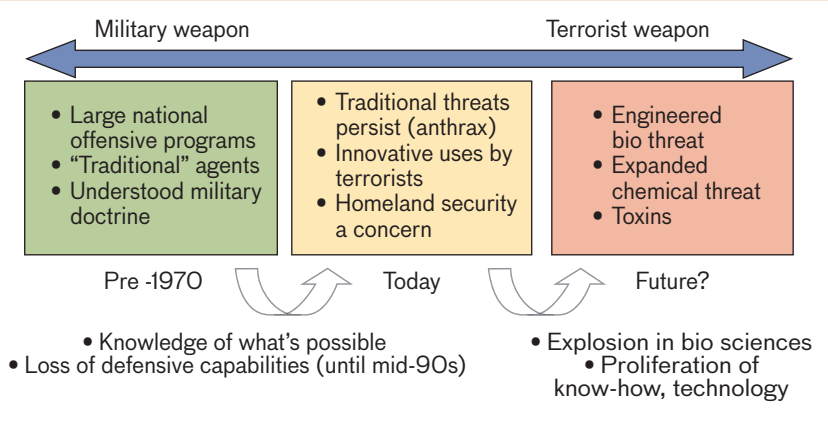

FIGURE A. **The threat of biological and chemical weapons has undergone considerable change over the past decades and continues to evolve, especially as microbiology and molecular biology advance. Today's threat looks much like that of the 1970s in the sense that terrorists are assumed to have the knowledge and the will to use chemical and biological weapons, and they will probably pursue the simplest path possible. The future threat is much more uncertain, with the potential for the creation of any microbe from scratch in DNA foundries.**

REFERENCE

a. R.J. Jackson, A.J. Ramsay. C.D. Christensen, S. Beaton, D.F. Hall, and I.A. Ramshaw, "Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox." *J. Virol.*, vol. 725, no. 3, 2001, pp. 1205–1210.

tests of integrated systems. This method and culture are embraced by other programs throughout the Laboratory, so they were easy to apply to chem–bio in a systems context. In this systems context, Lincoln Laboratory has been developing—on paper and in the field—integrated approaches to chemical and biological defense.

Historically, chem–bio defense has been a matter of deploying sensors and having a concept of operations to

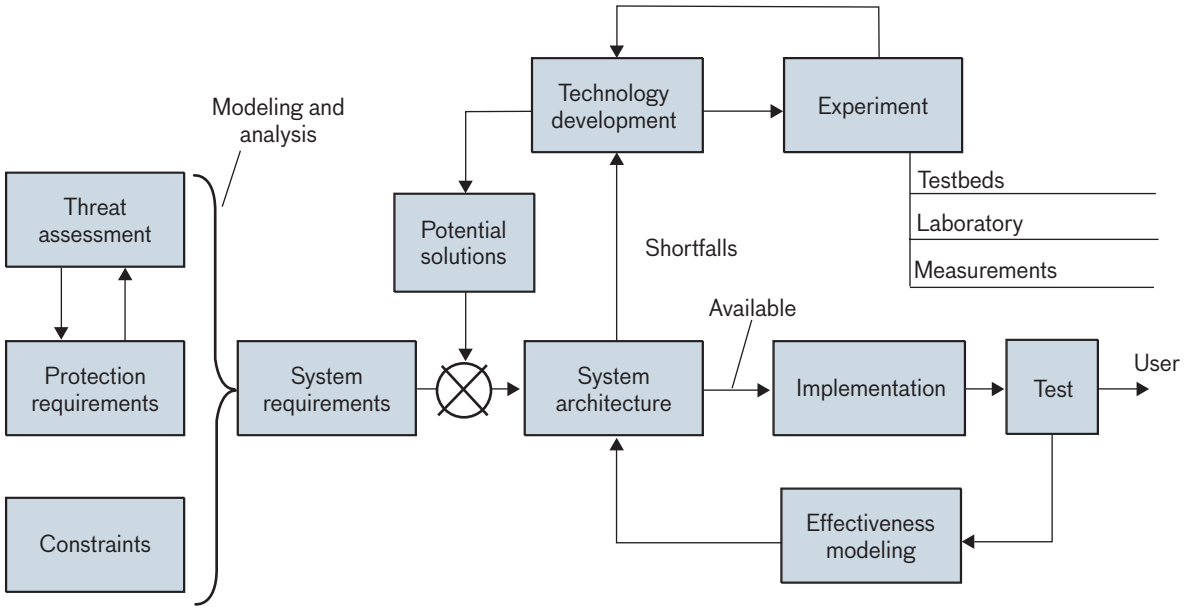

FIGURE 3. The capabilities-based technology development process begins, logically, with an assessment of requirements, based on part on threats and vulnerabilities. Other constraints, social, legal, and otherwise, are considered. This leads to a system strategy articulated in a set of requirements. Based on this, one or more system architectures can be postulated. If the components needed to effect the architecture are available, these should be used, thus producing the desired capability. If not, various technologies need to be developed and tested. The experimental phase of this development is an essential component, the success of which can lead to the new components being inserted into the architecture. Throughout, results are compared with predictions through a transparent, defensible analysis process.

respond to alarms from these sensors. A better way might be to fuse together sensor outputs with other known data (e.g., atmospheric conditions, threat conditions) and report to a user through a decision support process that takes into account various disparate information sources. Timothy Dasey and Jerome Braun report on efforts in sensor fusion and decision support for both homeland security and military force protection (page 153). What makes this problem different from many other information fusion efforts is the lack of realistic data—actual agent release cannot be done in the open air, real attacks almost never happen, and the probability of false alarm is significant. What we have here is thus a variant on the Maytag repairman problem: how to get ready for important events that almost never happen.

If a chemical or biological attack were to occur, then systems must be in place to minimize the dispersion of agent within the facilities where people congregate. As Daniel Cousins and Steven Campbell explain, building HVAC (heating, ventilation, and air conditioning) offers both vulnerability and a means of protection (page 131). On the one hand, a terrorist might take advantage of the building's air transport system to disseminate agent. On the other hand, the building's managers could use controls within the very same HVAC to protect the facility. Protection could involve use of detectors, filters, and air redirection. The key is to react in the least disruptive way; thus false alarms will be better tolerated.

Another question that we face is how to protect large populations against an aerosol attack of (for example) smallpox or anthrax over wide areas. Diane Jamrog and colleagues address vulnerabilities at the level of many thousands of victims and show the benefits of various detection and protection strategies (page 115). These strategies include environmental sensing and warning, medical diagnostics, rapid dissemination of treatment modalities, and recovery. Their models quantify, in a manner that policy makers can act on, an intuitive conclusion: The more quickly an attack can be accurately diagnosed, the more quickly treatment can be effected, and the fewer lives will be lost. The authors lay out a method whereby realistic protective measures can be put in place for the most worrisome scenarios. Their analysis also helps to define the necessary requirements for

sensing technology, thereby influencing other Lincoln Laboratory investments.

In their article on chem–bio defense (page 101), Adam Szpiro, Bernadette Johnson, and David Buckeridge address the potential advances in technology for diagnosing illness accurately and effectively. This medical surveillance work is based in part on a project led by Lincoln Laboratory several years ago called the Health Surveillance and Biodefense System (HSBS) study. The study's recommendations were simple: use accurate gene chips at the point of care to diagnose both common and illicitly caused disease (the common cold alongside anthrax), and communicate the results over a network. As straightforward as this may sound, and even though the necessary technologies are available, no such system yet exists. The HSBS study argued that the benefit to public health would far outweigh the cost of implementation (e.g., consider the multi-billions spent on inappropriate use of antibiotics). Though HSBS does not yet exist, this article reports progress in other efforts aimed at rapid signaling of a bio-attack based on health status reporting. In particular, Szpiro and colleagues describe the benefits of syndromic surveillance, wherein health-care professionals report the status of presenting patients to a correlating database. The authors also describe an innovative self-reporting approach to early warning, called BACTrack.

In short, the approach now being pursued and advocated by Lincoln Laboratory is strongly system-centric. We expect to continue to develop solutions to chemical and biological threats. We will do this by establishing an architectural framework that addresses specific and future needs, and by developing technology as needed to make these architectures possible. ■

BIBLIOGRAPHY

1. M. Dando, *Biological Warfare in the 21st Century*: *Biotechnology and the Proliferation of Biological Weapons* (Brassey's, London, 1994).
2. R.A. Falkenrath, R.D. Newman, and B.A. Thayer, *America's Achilles' Heel*: *Nuclear, Biological, and Chemical Terrorism and Covert Attacks* (BCSIA Studies in International Security, MIT Press, Cambridge, Mass., 1998).
3. J. Guillemin, *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism* (Columbia Univ. Press, New York, 2005).
4. Institute of Medicine and National Research Council, *Chemical and Biological Terrorism*: *Research and Development to Improve Civilian Medical Response* (National Academy Press, Washington, D.C., 1999).
5. J. Lederberg, ed., *Biological Weapons: Limiting the Threat* (BCSIA Studies in International Security, MIT Press, Cambridge, Mass., 1999).
6. A.J. Mauroni, *Chemical-Biological Defense, U.S. Military Policies and Decisions in the Gulf War* (Praeger, Westport, Conn., 1998).
7. R.A. Zilinskas, ed., *Biological Warfare: Modern Offense and Defense* (Lynne Rienner, London, 1999).

ABOUT THE AUTHOR

Darryl Greenwood heads Lincoln Laboratory's biological and chemical defense mission and is associate head of the Homeland Protection and Tactical Systems division. He earned his doctorate in electrical engineering from the University of Texas at Austin in 1971. Following four years in the Air Force, he joined Lincoln Laboratory in the applied radiation group. He has been a member of the Laboratory's senior management since 1985.