Technical and Policy Issues of Counterterrorism—A Primer for Physicists

No longer threatened by a rival superpower, the US now faces the growing danger of clandestine terrorist groups. Effectively countering terrorists requires that physicists actively contribute to the nation's defense.

Jay Davis and Don Prosnitz

From the development of radar and nuclear weapons during World War II to the creation of intercontinental ballistic missiles and deterrence theories during the cold war, physicists have played an essential role in defining US national security strategies and in executing the scientific programs that made those strategies successful. The US deterrence system, composed of theory, policy, and operational hardware, inhibited the Soviet Union until the cold war ended. Since then, that single geographically and ideologically focused opponent has been replaced by a multitude of state and nonstate actors armed with biological, chemical, and possibly nuclear weapons. The new national security climate does not diminish the need for physicists—it only changes the character of their contributions.

Several years ago, we both left technical jobs at Lawrence Livermore National Laboratory to help improve the federal government's response to threats posed by the dissemination of weapons of mass destruction and to improve domestic responses to them. (Davis was associate director for earth and environmental sciences at LLNL; Prosnitz was the chief scientist for the nonproliferation, arms control and international security directorate.) One of us (Davis) joined the Department of Defense with primary responsibilities overseas; the other (Prosnitz) joined the Department of Justice with primary responsibilities at home. We each provided a technical perspective on policy and operational options for conducting the war on terrorism. Naturally, we embraced technology as a means both to enhance present counterterrorism systems and to create new options for the ultimate decision makers. Persuading interagency working groups of the value of technological options became an essential part of our jobs. That often frustrating and occasionally rewarding process taught us the many possible roles for physicists in fighting terrorism. Equally important, we identified some of the behavioral attributes that increase one's ability to make a difference.

Understanding the problem

Although the term *terrorist* appears to have had its origin in the French Revolution, activities that we would clearly classify as terrorist date back at least to the Sicarii Zealots of the first century. And terrorism is not new to the US. The assassinations of several US presidents, bombings at such places as the University of Wisconsin and Oklahoma City, and the existence of the Ku Klux Klan, the Weathermen, and other homegrown terrorist groups are all part of US history.

What is new is the emerging capability of terrorists to cause harm that is qualitatively and quantitatively much more destructive than in the past. The threat the US is facing is not that of a lone madman, but of highly organized terrorist groups.

Chemical, biological, and nuclear capabilities are now within the reach of subnational groups. When such capabilities are married to global communication, transportation, and finance infrastructures, new threats to our national security are born. These threats are not simply due to the emergence of new terrorist groups or passing sociological trends. Long after Al Qaeda is removed from the scene, the threats will still exist. If the US is to reestablish its traditional level of security, the fundamental technical basis of the threat must be better understood.

The techniques that were used to counter the clearly defined enemy of the cold war will not defeat terrorism. Post–cold war terrorists have no single defined base of operations and no easily identified sponsor. Training and organizational activities can be carried out in countries where the people are wholly unaware of the activities under way within their borders. A 21st-century terrorist leader has a truly global span of control and action. Communication and fiscal transfers occur surreptitiously through use of the Internet and other systems and may pass below the threshold of detection by intelligence organizations. When terrorists are ready to act, they have the luxury of choosing the time, location, and means. As we learned on September 11th, the human, fiscal, and political consequences of the acts of a small group enabled by modern technologies and global infrastructure can be enormous.

Understanding the nature of the threat leads to some obvious strategies to counter it. US authorities must not try to defend all places at all times and should avoid focusing too much on the most recent attack. In the first case, the costs are simply too high. In the second, the terrorists will likely switch to a different means of attack after an initial success. Suicide bombings are an unpleasant exception to this assumption. Terrorists clearly find such bombings to be effective and repeatedly successful. Although suicide bombings are not a strategic threat, they are very difficult to deal with because of their impact on public perceptions and confidence.

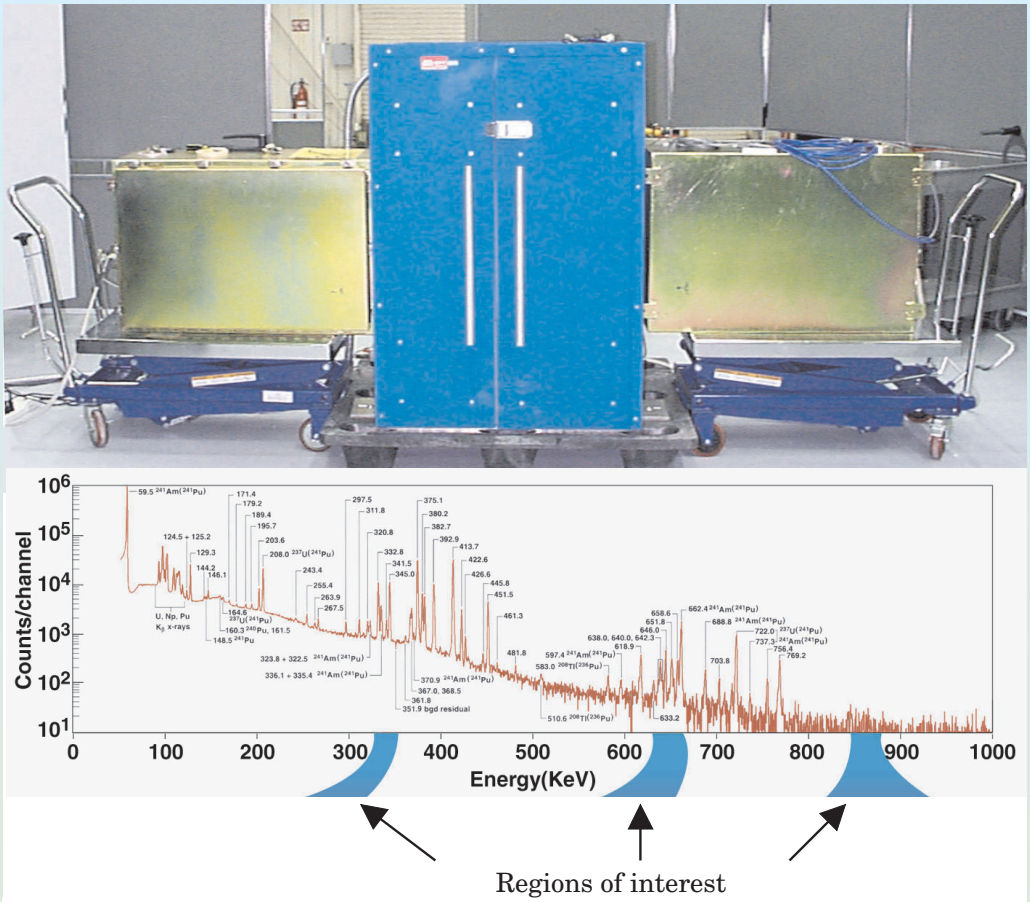
The asymmetric nature of the threat—that a few people can potentially cause harm to tens of thousands—mandates an essential element of any solution: the ability to identify and disrupt small, independent cells. However, counterterrorism activities carried out within the US are properly subject to many legal and policy constraints, and both privacy and civil rights must be protected. And the tactics used to fight terrorism should avoid both direct and

Jay Davis *is an experimental nuclear physicist who spent his career at Livermore as an accelerator and organization builder. He retired from the Livermore Laboratory in 2002.* **Don Prosnitz** *is a plasma physicist who has spent his career building lasers, accelerators and sensor systems of various types. He is currently deputy director for strategic plans in the homeland security office at Livermore.*

Box 1. Attribute Measurement Technologies

Nuclear weapons require a quantity of special nuclear material (typically either plutonium or highly enriched uranium) to wreak the destruction for which they are known. Measurement of the radiation emitted from the nuclear material is one of the most reliable ways of ascertaining that the material inside a weapon or storage container is of the type used in a nuclear weapon. Whether the concern is monitoring nuclear materials removed from Russian Federation military programs or identifying a smuggled nuclear device, radiation detection techniques can help determine if a particular item is suspect.

The rub with the radiation detection approach is that the information obtained by the measurements is inherently sensitive and reveals design and material details that provide important clues to how a weapon using them would function. To use this valuable information to make the desired determinations without divulging sensitive details, techniques have been developed that incorporate integrated software, hardware, and procedural features to prevent release of classified data and limit access to the minimum set of data required. These "attribute measurement" methods focus on specific characteristics of the item in question to determine if detected thresholds indicate a nuclear weapon, a component, or material without giving precise levels. Cooperative monitoring regimes between the US and the Russian Federation are a key context in which attribute measurement has been developed. In August 2000, the Department of Defense and Department of Energy sponsored an unclassified fissile material transparency technology demonstration for a Russian delegation at Los Alamos National Laboratory in New Mexico. That demonstration was hosted by the Defense Threat Reduction Agency and the lab under the cooperative threat-reduction program in conjunction with the Russian Federation's Mayak Fissile Material Storage Facility project.



The box contains the processing electronics that examine regions of interest in an object's gamma ray spectra (inset). The device also uses neutron counters to suggest the shape of the object. When the box is closed, none of this information is available. None is retained when the box is opened. Red and green lights on the outside of the box are the only indication whether an item has passed or failed.

During that demonstration, the Russian delegation observed measurements on several radioactive sources using an attribute measurement system with information barrier. The techniques involved measurement of gamma rays with a high-purity germanium detector and neutrons with helium-3 tubes configured in a version of a neutron multiplicity counter. Approaches were demonstrated for defining what attributes to look for to detect plutonium and to determine characteristics such as its mass, age, and whether it is of weapons grade. In addition to measurements on several unclassified authentication samples, the US delegation demonstrated to the Russian delegation a set of measurements using the information barrier system on a classified plutonium nuclear weapons component. The weapons component was kept in a sealed container while the measurements were performed. Significant development and review of information barrier concepts preceded the demonstration, both in the US and in Russia, and work is continuing to bring the technology to full maturity.

indirect economic costs. Seemingly obvious solutions to the terrorism problem fail when confronted with policy and legal requirements that can be, and often should be, as immutable as any law of nature.

Components of the solution

Physicists are taught that, to solve a problem, one must clearly understand what is being asked. Reaching that understanding often involves simplification by elimination of extraneous conditions. As the issues become clear and solutions evident, complications may be added. And the essence of the 21st-century terrorist threat, that a few can threaten so many, is the imbalance we must reverse.

However, the asymmetry can be overestimated. As a

Box 2. Securing the Borders

Even for those scientists who, intellectually, had long accepted that it was only a matter of time before the US suffered a grievous terrorist attack at home, the reality of September 11th was emotional in ways we could not have imagined. Like many others, I (Prosnitz) looked for ways to prevent such a horror from ever happening again. Unlike many others, I happened to be in a position in which I might be able to help. A few long weeks of hearing government agencies and commercial sectors describe all manner of vulnerabilities convinced me that the number of potential targets was enormous, and building impregnable defenses around each and every one impossible. Yes, we could do better—we are doing better—but we had to concentrate on people. We had to find and interdict those who would plan and execute future attacks. We had to control our borders.

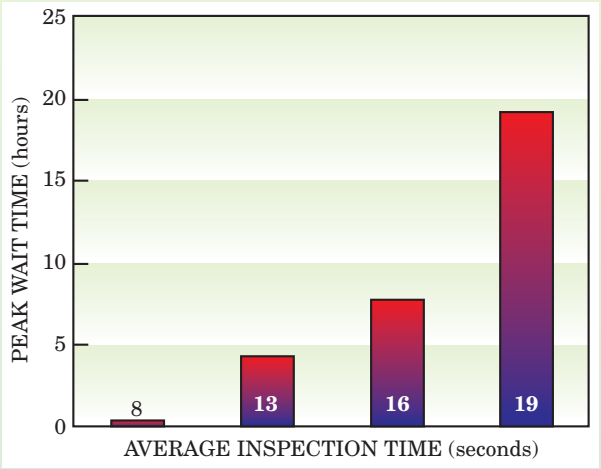
I started working with the Immigration and Naturalization Service (INS, which became part of the directorate of border and transportation security within the Department of Homeland Security on 1 March 2003). At first glance, controlling the borders appears to be a simple systems problem. Borders don't move and the visa process is designed to prescreen those who wish to enter the country. People are supposed to identify themselves at border checkpoints. A large law enforcement component supports the system, and multiagency watch list databases are available at ports of entry. But in reality, more than 540 million entry events occur each year at more than 420 ports of entry. Electronic databases are not always available and information is not complete. Airports, seaports, and land ports of entry have different constraints and service requirements. Visitors from around the globe carry a wide variety of documentation and are admitted under different entry requirements. If an inspector takes more than 10 or 15 seconds to make an entry decision, border traffic becomes gridlocked and the economies of our border cities and industries suffer. If more than 1.5% of those 540 million entries are referred to secondary inspection, border facilities quickly become overloaded, and traffic backs up. Enhancing physical security while impairing our economic security is a poor solution to a "simple systems problem."

Prosnitz

The Department of Justice put together a small team that included experts from the INS, the national laboratories, and outside technology consulting firms to look at, improve, and perhaps reengineer the entire system, from border queuing and biometrics to wireless technologies, database architecture, and data mining. As the team began its work, Congress passed the Patriot Act and the Border Security Act, laying out more border requirements.

As work progressed, we knew a systems approach would necessitate forming partnerships with the State Department's consular services and the Department of Treasury's customs division. Both of those agencies have a substantial stake in border control. Because intelligence and law enforcement agencies would provide "lookout" information, the system broadened. NIST and the FBI provided input on biometrics, and the Office of Homeland Security had additional policy input. Several nongovernmental organizations offered suggestions and cautions on how to facilitate commerce; it became clear that all of our neighbors and trading partners would have to be consulted. It also became clear that the advice of several international standards organizations, such as the International Organization for Standardization and the International Civil Aviation Organization, had to be considered. Border control quickly became a complex technical and political problem.

The story is not over. Agencies are cooperating, technologies are being evaluated, and cost and policy constraints are being balanced. If we are to succeed, it will be at least in part because a systems approach, not unfamiliar to "big physics," is being pursued.



nation, the US is only threatened physically and politically by multiple large-scale attacks. For a terrorist organization to mount such a campaign requires significant logistics and planning. A high-profile attack typically requires advanced surveillance, transport, weapons, financing, false documents, and overall planning and guidance. A defense strategy that forces the terrorists to use all of these resources not only makes an attack less likely to succeed, but increases the chances of uncovering the attack before it occurs. This strategy—forcing the terrorists to increase their signature while simultaneously developing better detection systems—is one that must be pursued. It is also important to make the successful execution of an attack even more difficult by deterring those who would provide shelter and resources to terrorists.

It is impossible to defend all places at all times, but a complete cycle of steps can be created that will require that terrorists assemble substantial assets in order to carry out a successful attack. This approach increases the chances of preventing terrorist acts and minimizes the social and human costs should an attack occur. The cycle consists of deterring supporters of terrorists, denying the assets needed to stage terrorist attacks, detecting and interdicting those who seek to commit terrorist acts, and managing crises and consequences. Attributing responsibility for an event, including those who provided direct support, followed by prosecution or retribution, closes the cycle by establishing deterrence. Each component of the cycle offers possible leverage of technology; each certainly contains policy, legal, and operational issues.

Deterrence is established by a clear governmental policy regarding the consequences of supporting terrorism or engaging in terrorist acts. For deterrence to succeed, it is essential that the US have a demonstrated will and capability to hold accountable those who are responsible for terrorist activities. Effective deterrent strategies must be designed around an understanding of what opponents of the US and, equally important, their supporters, hold

Box 3. An Operations Center Project: From Civil to Social Engineering

Davis

A responsibility of the Defense Threat Reduction Agency includes research to support, and assessments to evaluate, the security of US military installations against terrorist attacks. One of DTRA's precursor agencies held that responsibility as a result of the Khobar Towers bombing in Dhahran, Saudi Arabia, in 1996. DTRA activities range from sophisticated structural modeling to detonations of up to 2000 pounds of explosives targeted on a four-story test building at the White Sands Missile Range.

Early in my tenure as director of DTRA (Davis), it became apparent that a real vulnerability of base installations was the emergency operations center. If that is lost to an attack, the commander's ability to respond and recover is lost. Accordingly, DTRA looked for a project that would determine the costs of a sophisticated refit to guard against such threats. Jointly with the FBI, DTRA officials decided to outfit an emergency command center for the 2002 Salt Lake City Olympics so that it could operate through biological, chemical, or radiological terrorist attacks. Over a two-year period before the Olympics, we refitted 50 000 square feet of leased space with emergency power, positive-pressure air-handling equipment, internal threat detectors, and decontamination capabilities. Most important, a second emergency operations center was created where the more than 40 agencies supporting security and health at the Olympics could work together with computer databases and situational awareness tools to achieve common understanding of threat events.

This project began as a civil engineering exploration: What could be done, what would it cost, and what knowledge could be gained to improve military force protection? It ended as a great success of social engineering across the boundaries of many organizations that frequently have authority, turf, and resource conflicts. By being the honest broker in a supporting role and the willing bill-payer for a $25 million project, DTRA created an atmosphere in which the multiple players were much better integrated than at previous major events. We extracted the engineering and cost information for future application with more sophisticated technologies, but the lasting product was learning how to build effective operational relationships.

dear. On this point, sociology assumes an importance equal to technology.

Of paramount importance to the war on terrorism is the denial of the tools of terrorism—especially weapons of mass destruction—to terrorists. Techniques of denial may range from the simple—better guards and fences—to technologically complex steps that include chemical weapons demilitarization, plutonium segregation and storage, and enriched uranium blending. Denial may also include technically and politically exotic techniques such as attribute determination performed on the Russian weapons-grade plutonium, as discussed in box 1 on page 40.

The ability of the US to detect potential threats has received a great deal of attention since September 11th. In a counterterrorism context, detection is broadly defined as techniques used to identify materials and individuals moving in and out of regions where terrorists are based, or toward potential targets. Methods to better defend US borders are discussed in box 2 on page 41. Activities involved in detection include finding indications and warnings of terrorist planning through the use of advanced information systems and analysis. Detection is enhanced both by forcing the enemy to use large infrastructures and by sorting out minor crimes from true national security threats. If detection is successful and produces "actionable intelligence," it can lead to interdiction using means up to and including force to prevent the planned event from occurring.

Crisis management consists of steps to minimize effects during terrorist attacks. Those steps range from immunizing all or part of the population (for example, first responders and medical personnel), to actively managing air-handling systems in large buildings. For more details, see box 3 on this page.

Consequence management involves the steps to mitigate damage from an attack and speed recovery. Technical components include having in place predictive codes for dosimetry, decontamination technologies, triage, and population management experts. Effective public communication and the associated psychological treatment of victims are important components of successful consequence management. Providing accurate information to people affected by an event is essential if the information is to be trusted and acted upon. Education and practice before an attack are necessary to instill knowledge and establish trust.

Attribution of the event is necessary to establish responsibility and to choose between a judicial or a military remedy. The future will likely bring multiple terrorist attacks and the public can be reassured only if it believes there is an aggressive, effective effort to catch the perpetrators and prevent future attacks. In the political and emotional aftermath of a major attack, quickly ruling out possible perpetrators may be as important as identifying the terrorists. Attribution capabilities close the circle by supporting deterrence and hence are vital and require considerable investment. Physicists and their traditional tools used in perhaps untraditional ways, have a great deal to offer in identifying the responsible parties. Some of the methods of identifying the sources of biological terrorism are discussed in box 4 on page 43.

How do physicists contribute?

Our positive experiences in Washington, DC, demonstrate that physicists have much to contribute to homeland security. As a group, physicists are inherently comfortable with complex systems problems and recognize that a silver bullet rarely exists for complex problems. Most physicists insist on quantitative analyses of problems and, as a result of project management experience, are comfortable and facile with having to make trades across disciplines.

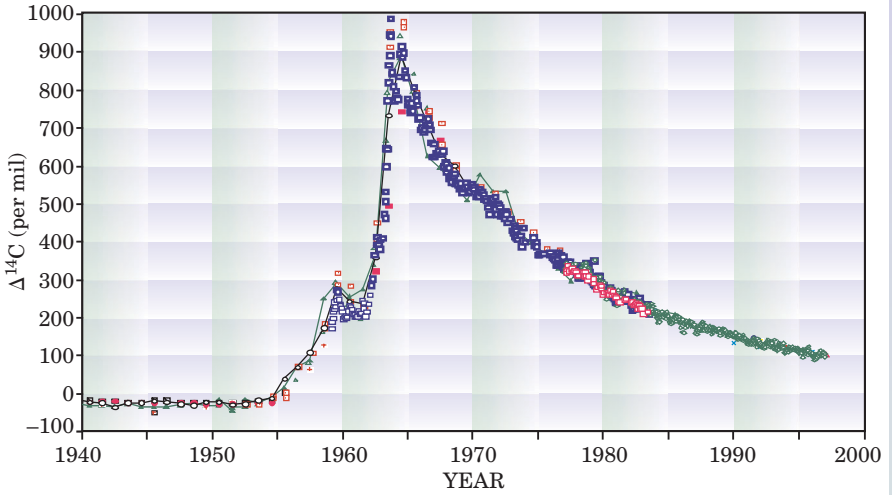
Technologies developed by applied physicists not only have played a role in defense, but have made major contributions to the explosion of manipulative, analytical, and characterization technologies in the biosciences, chemical sciences, information sciences, and materials sciences. Applied physicists have become a diverse community linking and supporting other disciplines. It is precisely this last skill, linking multiple disciplines that will lead to success in countering the new threats to our security.

Challenges and investments

The positive identification of individuals crossing US borders is critical to detecting and deterring terrorist acts. Complete defense of the vast US borders against illegal entries is currently impossible. Subject to economic and political costs, technical means such as biometrics and

Box 4. Determining the Age of Biological Agents

The analysis of isotopes contained in biological agents can yield information on their point of origin, conditions of culture, and time of production. Traditional carbon dating relies on the radioactive decay of carbon-14, which permits dating of organic materials that are at least a few hundred years old. However, relatively large amounts of ^{14}C-labeled carbon dioxide were created during atmospheric nuclear tests in the 1950s and early 1960s (see ref. 1 for example). The decline of ^{14}C reflects the incorporation of the carbon dioxide into the biosphere since the cessation of above-ground testing. This rise and fall of ^{14}C remains measurable in the biosphere, and accordingly, ^{14}C concentrations in materials such as illicit drugs and biological weapons can be matched to this "bomb curve" to assess the average age of their plant and animal starting materials.



The atmospheric concentration of carbon-14 worldwide doubled as a result of above-ground nuclear testing.

Because concentrations of ^{14}C are exceedingly low, about one part in a trillion in environmental samples, only accelerator physics technologies can resolve and quantify such low isotopic abundance's in small samples. Accelerator mass spectrometry (AMS) was originally developed because archaeologists needed a method superior to decay counting for precise measurement of ^{14}C. AMS systems use traditional mass spectrometry methods coupled with a particle accelerator to accelerate ions to energies sufficient for destruction of molecular isobars that would otherwise interfere with the measurement of the isotope of interest. AMS is now the standard method for radiocarbon dating and is ideally suited for forensic determinations of ^{14}C because of its precision and ability to process amounts of material less than 1mg, for example.

The use of AMS to determine the age of biological samples assumes that the calendar ages assigned to the results of these analyses reflect isotopic equilibrium with the organism's growth medium, and that the growth medium represents an average age of its constituents. Due to the fact that a ^{14}C concentration intercepts the bomb curve on both its upward and downward slopes, dates derived by this method have two values. Choosing between them requires other data.

Isotopic ^{14}C signatures may also make it possible to discern between several samples grown on the same medium. For example, cultures grown on media that were produced at different times would have different ^{14}C contents. Therefore, it may be possible to discriminate genetically identical organisms by their ^{14}C signatures.

"high-tech" identification cards can make it easier for authorities to positively identify people traveling across borders. Such cards, supported by border inspectors who have access to visa databases, can help create a "smart border" that will simultaneously expedite commerce and enhance domestic security. Border solutions must work for all modes of travel—pedestrian, bicycle, car, truck, train, boat, and airplane—and for all ages and nationalities. The system must function 24 hours a day, 7 days a week in all climates and must respond to alerts in seconds, not minutes. New systems cannot be limited to official ports of entry. Better surveillance is needed along the entire border to deter those who would attempt to enter illegally. The current range of unattended sensors is measured in tens of meters; the border is measured in thousands of kilometers.

Close scrutiny of materials crossing either national boundaries or security perimeters within the country is also critical. Protective screening techniques range from simple radiation detectors, which are already in the hands of border inspectors and overseas customs agents, to scanners for the millions of cargo containers that enter the US annually. Cost, effectiveness, and reliability are crucial in those efforts. Containers might be effectively inspected by placing small detectors in each one, essentially creating smart containers as an alternative to elaborate port-based inspection systems. Sensors integrated into containers have days or weeks to monitor for proscribed materials rather than minutes in the ports. Smart containers may offer additional economic value in terms of product security and environmental control during shipping, and hence be seen as a benefit rather than a cost. Such systems obviously must be cheap and rugged. And with 16 million containers per year crossing US borders and port productivity a vital factor in economic competitiveness, the false alarm rate must be very low. Perfect security for all cargo containers moving through the world's ports is not achievable, but increasing the risk and cost of attempting to bring materials for weapons of mass destruction into the US is a valuable and effective deterrent.

Systems that provide indications and warning are particularly vital in minimizing the effects of biological agents. If an agent is dispersed covertly, the attack will only be detected when victims exhibit disease symptoms. In such an event, the resulting outbreak could overwhelm local medical response personnel with devastating results. The ultimate goal is to detect a biological agent in time to warn the public, not just treat the victims. Any credible near-term plan must be a mix of improved medical surveillance and active detection systems. DNA recognition and amplification by polymerase chain reaction techniques, and physics-based techniques such as aerosol sorting, photodissociation, and mass spectrometric analysis of molecular signatures, will likely be used in such detector systems. Other than the actual transducer, most components of a biodetection system are modern instruments of

exactly the type experimental physicists have been designing for years.

Integrating distributed sensors to reduce false positives and other extraneous signals is also a technique long used by physicists. Creating a first-rate surveillance and detection system will involve multidisciplinary technological tradeoffs as well as sociological and economic considerations. Clearly, many of the analytical tools and system architectures are familiar to physicists.

Of particular importance in dealing with the consequences of any terrorist event are the predictions of the dispersal, deposition, and consequences—both immediate and delayed—of any release of radioactive, chemical, or biological agent. Both the US Department of Energy and the Department of Defense have dispersion modeling capabilities and programs to test and improve the predictive powers of those models. Although the models perform well in open terrain, much more work needs to be done to predict dispersal in urban environments. Cities have complex microclimates driven by temperature, humidity, and highly variable wind patterns caused by tall buildings.

The models must be accurate enough that first responders know how to stage their response, establish shelter zones, and determine the best evacuation routes. The ability to acquire real source data early in an event, insert the data into the simulation, and then produce multiple models of the event is critical. Accurate data and predictive models allow those responding to a terrorist event to make decisions with a reasonable degree of confidence. Again, the technical role of physicists is obvious. The educational and interpretive roles may be less obvious, but are no less important.

Part of the educational role in the war on terrorism is the creation of scenarios that can be used to test interagency relationships and practice responses across organizational lines. A central dilemma is that counterterrorist training is expensive and time consuming. Police, fire, public health, and other first responders have "day jobs" that are their primary responsibilities. Few cities can spare their frontline emergency personnel for extensive counterterrorism training, so training methods that are both time and cost effective are needed. Scenario play—the civilian equivalent of military war games—is essential to develop trust, authority, and communication across organizational lines. Running scenarios assesses not only responses to events, but also the quality of previous R&D investments, intelligence activities, and training. Gaming often elucidates gaps that can be filled by focused R&D.

Heavily weighted toward physics tools, the prediction of weapons effects helps create model scenarios and makes them credible. Physicists are most useful when they can assure that all aspects of a scenario are accurate. The lessons learned span resource management, medical care, communications, and the overtly political and psychological aspects involved in responding to an attack. By participating in the scenarios, physicists also become more familiar with the difficulties in communicating with nontechnical emergency managers and see, firsthand, all aspects of a mass casualty event.

Physics skills are required to develop the technological, operational, and decisional capabilities needed for the rapid attribution of nuclear and biological terrorist acts. If a nuclear attack should occur, database connections, sample acquisition, measurement capabilities, and knowledge of and access to design, explosion, and nuclear reaction codes of nuclear weapons will be essential in tracing the source of a detonated weapon. To that end, the Defense Threat Reduction Agency (DTRA) began a formal program of nuclear forensics in 2001.

In a biological attack, much of the information about weaponization, characterization, dispersion patterns, and distribution history of a biological agent will come from the tools of physics. Lessons learned from the current anthrax investigation suggest that a formal program similar to DTRA's nuclear forensics effort is needed for biological threats, and the FBI is working with the Department of Homeland Security to establish just such a program. It will encompass an all-discipline approach to plant, animal, and human pathogen forensic research and development and, of utmost importance, will include strict validation of all laboratory techniques.

These are immensely difficult forensic problems and technologists have a responsibility to define the "art of the possible." Leaving the political community unaware of the scope, precision, and uncertainty of physicists' capabilities would be as irresponsible as misleading them about the omnipotence of technical solutions. In the event of nuclear or large-scale biological terrorism, the political pressures for attribution—and the consequences of misattribution—will be enormous. Crisp operational plans, including technical procedures, are essential for an effective response. A formal decision-making system that enables an accurate interpretation of what occurred is also necessary. The system will likely have to address the decision of how best to pursue the perpetrators and, ultimately, if a judicial or more forceful military response is required. The technical community must be prepared to step forward and provide the absolute best it has to the nation's leaders.

How have we done?

We two authors feel that our years invested in the government have been fruitful and rewarding, and we hope our contributions have left the country better prepared for a challenging future. We've learned that physicists can still slide across disciplinary boundaries; that they can make contributions to difficult issues coupling policy, operations, and technology; and that our reflexive systems approach serves us well in multidisciplinary and multiorganizational problems. We've also learned that the policy and operational segments of the military, intelligence, public health, law enforcement, and other first responder groups are eager for our support in their battle against terrorism. It is clear that emerging terrorist threats are as daunting as those of the cold war. They will not be solved quickly, but they will be solved. Reestablishing the means and theory of deterrence, and of detecting and stopping terrorists, is a task that demands and requires the participation of physicists.

Reference

1. I. Levin, B. Kromer, *Radiocarbon* **39**, 205 (1997). ■