Detection of Biological Agents Used for Terrorism: Are We Ready?

Countering the use of biological agents (biothreats) requires a complex network of intelligence, detectors, laboratories, and the personnel and facilities to treat exposed individuals. In October 2009, 8 years after the mailing of letters containing Bacillus anthracis, the causative agent of anthrax, the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism released an interim report asserting that the US is failing to address biological weapon proliferation and biological terrorism. The Commission Vice Chairman, Jim Talent, stated in that report that “It is only getting easier and cheaper to develop and use biological weapons—and our best defense is to mitigate the effects through faster, safer vaccines and therapeutics.” It is important to remember, however, that the decisions to administer vaccines and therapeutics require robust tools for the detection and identification of biological agents. The capabilities of current detection technology have been a limiting factor in creating a thorough process to deal with biological threats, and the matter is complicated even further by the almost infinite types of sample matrices and potential contaminants that confound analytical processes. Although technology and capabilities have improved since 2001, the majority of available devices are still based on chromatographic immunoassays, PCR, and ELISA. Newer, potentially faster and more sensitive technologies based on concepts such as nanowires, quantum dots, microcantilevers, and hand-held spectrometers are reported to be available or near availability, but most still require significant amounts of testing and validation under conditions replicating actual use. In this Q&A, 3 experts in the field of bioweapon detection answer questions about the current status of biothreat detection technology.

From your perspective, please explain the difference between biothreat detection and biothreat identification.

Mark Hollis2: Biothreat detection can happen in 2 ways: (1) people, animals, and/or plants fall ill in such a pattern that a biothreat can be suspected, and/or (2) the biothreat is identified via one or more identification tests before illness occurs. True biothreat detection cannot be done without a good determination that the organism or toxin is pathological. For testing, this usually demands identification of the organism or toxin, at least to the level of specificity that says with high probability that it looks like one that is known to cause illness. There are several classes of biothreat “detectors” available that do not do true identification but nevertheless have some utility in an overall detection system. Some are merely aerosol particle counters, and can only say that the density of particles in the air has risen but cannot discriminate biological from nonbiological. A better class of detectors senses UV-stimulated fluorescence; some are capable of classifying particles as biological vs nonbiological but cannot tell, for example, the difference between benign and pathogenic bacteria. These detectors are typically fast (approximately 1-min response) and are often used as front-end triggers in a layered system of sensors that employs slower but more specific identifiers to examine the samples further. True biothreat identification has historically been done in public-health laboratories where a range of techniques is used from the approximately 120-year-old culture methods of Koch and Pasteur to modern immunoassays, PCR amplification and sequence detection of DNA, and mass spectrometry. These methods can be quite definitive, but a high-certainty characterization of a pathogen can take 2 or more working days using them. Over the last 15 years faster, more compact versions of immunoassays, PCR analysis, and mass spectrometry have been migrating to the field where some are now used as second- or third-stage identifiers in the layered system concept above.
may also include optical sensing. After a trigger detects the number of particles in a certain size range increases. It is presumed attack. Preparations must be implemented to reduce the impact of a potential biological threat or not. Then there are basically rapid immunoassays, which are very similar to home pregnancy tests, or comparable methodologies. There are some mobile molecular techniques such as PCR that are out in the field. Although my feeling is that mobile PCR in the field should be performed only by highly trained individuals and not just anyone. Running a home pregnancy test is a lot different than running a PCR. In the laboratory, you have those same methods used to identify those biothreats—both in the field, like what first-responders would use, and also perhaps in a public health laboratory at a higher technology level.

Cheryl Gauthier: The predominant technologies used by first responders to detect biothreat agents in the field are (a) protein kits that test for the presence of protein as an indicator of a possible biological agent, but are not specific to bacteria or biothreat agents; (b) pH measurements to determine if the substance is acidic, basic, or neutral; (c) spore detectors that detect the presence of any and all spores, but are not specific to a spore-forming biothreat agent; (d) metabolic assays that detect enzymes such as catalase to indicate the presence of bacteria, but are not specific to biothreat agents; (e) immunoassays such as HHAs that detect target antigens specific to biothreat agents; and (f) molecular assays that detect biothreat agent DNA, some of which may be multiplexed to detect more than one biothreat agent at a time.

The predominant technologies used to detect and identify biothreat agents in public health laboratories are (a) culture/biochemical reactions, (b) ELISAs that detect a specific target antigen, and (c) molecular assays that detect specific DNA sequences.

Tom O’Brien: The first line would be generic tests that look for things like proteins that say yes, there’s a potential biological threat or not. Then there are basically rapid immunoassays, which are very similar to home pregnancy tests, or comparable methodologies. There are some mobile molecular techniques such as PCR that are out in the field. Although my feeling is that mobile PCR in the field should be performed only by highly trained individuals and not just anyone. Running a home pregnancy test is a lot different than running a PCR. In the laboratory, you have those same methods used to identify those biothreats—both in the field, like what first-responders would use, and also perhaps in a public health laboratory at a higher technology level.

Cheryl Gauthier: When I think biothreat detection, the first thing that comes to mind is a presumptive test, of the type that is most often used in the field and is generally not as sensitive or specific as a laboratory biothreat identification system. In terms of detection equipment, a device can be as simple as a hand-held assay (HHA) which generates a qualitative result or as complex as a portable PCR machine that reports a quantitative value. An example of an emerging technology in detection is automated fixed detection systems, which may soon be deployed in businesses or large facilities. In this case the system acts sort of as a “biological smoke detector” and will alarm if there is a biological release inside a building. Biothreat identification, on the other hand, is a far more specific and complex process. This is not a presumptive test but a confirmatory test because you have proven through very sensitive and precise laboratory methods that a specific agent is present. Depending on whether you are dealing with bacteria, toxin, or virus this “confirmation” is achieved through the use of cultural, biochemical, or molecular methods or by sensitive immunoassays. Public health preparedness programs seek to define thresholds at which results become “actionable,” when interventions must be implemented to reduce the impact of a presumed attack.

Tom O’Brien: Biodetection is a generic term for identifying something out there that is biological. But it can be very nonspecific like pollen, yeast, volatile organics, or a real threat. In the military they call that a trigger: it senses when a number of particles in a certain size range increases. It may also include optical sensing. After a trigger detects something, another device is used to identify if a threat is present. These devices look for a specific biological signature for things like anthrax or plague. One identifies the organism, one detects a biological threat in general. In general, one detects a possible threat, the other identifies specific threats. This also keeps costs down. Detection devices and reagents are usually more inexpensive than identification techniques.
types of techniques, in more sophisticated devices and equipment, plus the ability to culture things to see if they’re alive. These tests typically take a little bit longer, and are more sensitive and specific than field assays. In reference laboratories, I prefer multiple devices and techniques to increase accuracy. You want to see both molecular targets and immunological targets identified. And now things like mass spectroscopy are coming on board in the laboratories. I was one of the founders of the US Navy’s first Bio-Defense Program which is now called the Biological Defense Research Directorate (BDRD) created after the First Gulf War because the rapid tests used in that war were very unreliable. There, we were one of the first laboratories to believe in “confirmatory analysis.” This term was first coined by Capt (Ret) James Burans who is now the director of the National Biodefense Analysis and Countermeasures Center (NBACC). Confirmatory analysis combines immunological, molecular, and culture methods. We also transitioned this concept into a mobile laboratory that had an alert time of 3 h to get to the airport. We brought this laboratory to Iraq for the Countermeasures Center (NBACC). Confirmatory analysis combines immunological, molecular, and culture methods. We also transitioned this concept into a mobile laboratory that had an alert time of 3 h to get to the airport. We brought this laboratory to Iraq for the United Nations and identified weaponized biothreats. We tested the bomb at the Atlanta Olympics and were present at things like G7 meetings and national political conventions.

Mark Hollis: (a) For first responders there are 2 main classes available: (1) so-called immunoassay tickets that use the same format as a home pregnancy test but incorporate antibodies on the wicking strip that bind to epitopes of pathogenic organisms or toxins, and (2) fast, portable PCR instruments. The immunoassay tickets provide a result in <20 min and the field PCR instruments provide results in under 1–2 h, depending on the instrument and how much sample preparation is required. First responders often use infrared (IR) or Raman-based optical sensors, which are very useful for chemical detection and which can provide limited classification for some biological materials, but not true identification. (b) I briefly described the public-health laboratory methods above in my response to the first question.

From a strategic standpoint, a system to counter a biological attack would be based on a “detect to warn” principle. Please explain the idea of detect to warn, and do we have this capability today?

Mark Hollis: “Detect to warn” means that one can detect a biological attack fast enough that response measures could be taken to prevent many or all of the subject population from getting infected. For aerosol attacks, response measures include such things as masking, shutting down HVAC (heating, ventilating, air conditioning) systems, leaving the area, and/or attacking the attacker before the pathogens can be released. For food or water attacks, the main response would be to prevent consumption of the contaminated material.

Detect to warn is very difficult for many types of biological attacks since for many pathogens it takes only a few pathogen particles to infect, which can be inhaled or ingested in just a few minutes. Therefore, for building protection, detect-to-warn sensor systems must be really fast and initiate their responses in under 5 min. Detect-to-warn capability is available today in only a few special facilities. For food or water attacks, the detection timeline can be extended, depending on the point in the production/consumption chain at which the detection is employed. However, as evidenced by the recent episodes of contaminated food reaching consumers (Salmonella on raw tomatoes, E. coli on spinach), our current system of monitoring food safety is not a robust detect-to-warn system.

Cheryl Gauthier: “Detect to warn” refers to the ability to detect an agent quickly to provide warning and take protective actions; it does not “prevent” an attack. As far as applying the detect-to-warn principle to prevent an attack, there is some capability with respect to intelligence gathering, but not with respect to analytical capability. Existing detect-to-warn systems, such as the US Postal Service (USPS) Biohazard Detection System (BDS), can provide early warning of a release but do not prevent an attack or release.

One aspect of the response to prevent bioterrorism has been the fielding of “kits” for first responders (firefighters, police, etc.) to test for the presence of and identify biothreat agents. How good are these kits, and do they really provide a robust system to detect and identify a biological threat?

Cheryl Gauthier: While response plans do exist, the national objectives of field detection have never been clearly defined. While many first responders have and use these kits, there has been no direction as to when, where, and how they should use them. For example, what exactly is the role of the first responder in a bioterrorism event? Do first responders really need field kits for biodetection? How reliable and accurate do the field kits need to be? What actions will be taken based on the results from a field kit? The field kits currently available to first responders have not been proven to possess high sensitivity and specificity and are subject to variable rates of false-positive and false-negative results. Thus the reliability of these field kits or devices is far less than the technology used at a Laboratory Response Network (LRN)-approved laboratory. Any reliance on the results from these devices carries a risk that unnecessary actions may be taken on a false-
positive result, or that no actions will be taken on a false-negative result. While some urge the need for improved biodetection capability, there is still not a national strategy outlining where field biodetection fits in, with its inherent limitations and uncertain objectives or purpose. Contrary to some misperceptions and based on the information above, the purpose of field kits for first responders should not be to identify a biothreat agent. This is an operation that can only be performed by an LRN laboratory. However, information gained from these devices, if employed properly, can be used as one part of an initial risk assessment to provide justified support for short-term tactical decisions such as (a) securing a building and denying reoccupancy, (b) holding first responders and hazardous material (HazMat) teams on scene, (c) prioritizing the transport and testing of samples at an LRN laboratory, (d) accounting for potentially exposed individuals, and (e) providing public health officials and public policy makers with knowledge of the increased potential of a credible event. Even as the current technology improves, that alone is not enough to ensure that you will have a robust system to detect and identify a biological threat. You will also need (a) a coordinated and accepted national strategy for the response to a bioterrorism event; (b) guidance on acceptable levels of detection, sensitivity, and specificity as they relate to risk of disease; (c) independent evaluation of field kits and devices to ensure that they perform according to manufacturer’s claims and achieve consensus-derived acceptable levels of detection; (d) routine maintenance on the equipment to ensure that the equipment is functioning properly; (e) training of personnel to a national standard and annual demonstration of proficiency/competency to guarantee that the first responder using the equipment is competent to do so; and (f) active and robust channels of communication between responders, the LRN laboratory, the Federal Bureau of Investigation (FBI), and other law enforcement and public safety agencies.

Tom O'Brien: Before founding Tetracore, at BDRP, we developed the HHAs, which are just like home pregnancy tests—immunoassays that the military is still depending on for multiple biothreat identification scenarios. These tests were used in Senator Daschle’s office and the result of that test definitely increased the importance of the testing that followed and the response that followed. I’ve always felt that since HazMat teams have tests for chemicals, radiological, and nuclear threats, they should also have tests for biothreats. However, the quality of the immunoassay-based devices is only as good as the antibodies. While at the BDRP, we also initiated the Critical Reagents Program (CRP) to address that issue. In my opinion, the LRN is okay if you have 1 or 2 samples, and they can turn that around pretty quickly. But if something like the 9/11 events or the anthrax letters happens again, and every team in the country is collecting 300 samples a month, will they really turn those answers around in a day? I know that they were collecting that much in local counties around DC following the anthrax letters. Does the LRN have the personnel and reagents in place in every lab? I don’t know, you have to ask the LRN that question. The HazMat teams are qualified and they understand that these are screening tests, it’s part of the protocol to send it off to the LRN anyway. They’re not going to go off the deep end for a false positive. They’re going to follow protocol. I believe first-responders use biothreat detection as a tool in the toolbox. They’re not the be-all end-all. Many of the laboratory communities are against the practice, and I don’t understand why. People run pregnancy tests many times every day in the US and nobody looks down at these the way they look down at rapid tests in the bioterror threat community.

However, to be quite honest, when my kid gets a rapid strep or flu test at the doctor, and I look at my kid, and he looks sick, and they say it was negative, I take it with a grain of salt. People expect 99.999% sensitivity for a screening test, and nothing is like that. Some of the chemical tests out there are 70% sensitive, and nobody’s screaming about them. I don’t know why they’re so against these things. And then, there’s the sensitivity issue, people talk about an infectious dose that goes down to 100 spores or so. Well you have got to breathe those spores in. Sensitivity and infectivity should not be compared. It is irrational. The amount that was in one of the anthrax letters would have killed all of Washington, DC, by that theory. People don’t call 911 for a microgram of spores. You can’t find that in my office if I put it somewhere. Nobody is going to find a little powder of anthrax. All you have to do to get these rapid detection devices to light up is to touch a swab, dry or wet, to a powder, and put it into a solution.

Mark Hollis: There are 2 categories of inexpensive kits in common use: a rapid protein test that can determine that the material is biological (but not identify it), and the immunoassay tickets described above. The false-positive and false-negative rates of the immunoassay tickets under ideal laboratory conditions are a few percent or better for sample concentrations $>10^4$ colony-forming units (cfu)/mL, but for real-world samples they can be worse due to contamination of the sample by environmental residues, soils, etc. A more expensive capability that many first responders now have is field- portable fast PCR. Reports indicate that the false-positive rate for field PCR is quite low, but that the false-negative rate can be higher due to PCR inhibition caused by environmental contaminants. PCR vendors
typically recommend some type of sample preparation to minimize false negatives, but further improvements are still needed.

Following the 2001 Anthrax attacks there have been several “new” technologies touted to solve the complex problem of biothreat identification. Yet 8 years later few if any of these seem to be commercially available. Why do you think these technologies have failed to materialize?

Tom O’Brien: It’s probably a money and a time issue. Typical clinical biosensor devices take years and years and millions and millions of funding to get to the diagnostic laboratory, let alone getting to a portable unit that a nonclinician could use. Money went into these things, to miniaturize them and get them out the door. But, as 9/11 fades in memory, funding has gone down, both from the federal level to develop them and from the local level to purchase them. You could develop a great device, but it might cost $9000 and the local HazMat team doesn’t have $9000 anymore. Since there is a lack of funds to get some of these things out the door, and a lack of funds to buy them, from a business standpoint, it doesn’t make a lot of sense to spend internal time and funds for development.

Cheryl Gauthier: Three reasons that occur in combination: (1) Without acceptable standards and independent third-party validation of these devices, they are no more accepted than the current technologies as far as accuracy and reliability; (2) There is some degree of market saturation and fatigue over the issue; (3) The newer technologies are expensive and federal funds are decreasing. Without good reason to invest in new technology (i.e., acceptance of a strategy and use of these devices), the available money is being directed to other needs.

Mark Hollis: There is often a lot of hype in the technology-development world when a new threat emerges, i.e., people trying to bend “their technology” to make it fit a new market. There have been literally hundreds of reports of new technologies that claim to offer benefit for this problem, most of which are still at the basic-research stage in universities. The reasons that few are now in the marketplace often involve the fact that the technology requires more development than the developer thinks, or that the developer does not truly appreciate all the demands of the application in the field. In addition, the road to the marketplace for a new technology has many nontechnical roadblocks such as patenting, licensing, commercial financing, manufacturing scale-up, etc.

In your opinion, what do you think is the biggest hurdle to deploying a biothreat detection and identification system in the US?

Mark Hollis: To truly prevent any attack on US soil, one would need a massive array of detect-to-warn systems in every major building and complex in the country coupled with an outstanding intelligence-gathering capability just devoted to bioweapons. As with most things of this scale, this requires that the threat be viewed as serious enough to merit the large expenditure over and against competing national priorities such as regular healthcare, mainline defense, border security, education, etc.

Cheryl Gauthier: Prevention will be difficult to achieve in the context of a biothreat detection and identification system. Once you’ve detected a release, the attack has already occurred, so how can or could you have prevented it? Biothreat detection and identification can be used only to provide early and accurate warning and to expedite effective mitigation. Additionally, averting an attack on US soil is not dependent on a single hurdle, but rather close coordination between deterrence, intelligence, and interdiction. As the national focus shifts from the negative aspects of biothreat detection devices to a coordinated biothreat response strategy we begin to address some of the past hurdles. This broader focus puts achievable objectives in sight and allows us to work together to gain experience and confidence in our collective capability. It’s important to remember that a critical element of terrorism is the erosion of public confidence in government’s ability to protect us. Agreeing on a strategy, and collective movement toward that strategy, puts us in a much better position to reassure the public and most importantly to protect the public.

Tom O’Brien: Cost. Period. To cover every major city, every 10 blocks, just the amount of energy and people is prohibitive. I don’t know if you will ever get complete coverage. I just don’t see that happening. Even just covering major transportation sites is an enormous cost. In general, could this money be better spent with regard to our nation’s overall safety and health?

Do you have any additional comments?

Mark Hollis: Detect-to-warn systems have been effectively demonstrated for building and site protection, but are in very limited use right now. I believe that their installation should be expanded to many high-risk or high-value facilities over the next several years, but that will take a renewed awareness of the seriousness of the threats, an awareness of what these systems can do, and
the financial ability and political will to put them in place.

**Tom O’Brien:** Just in general, we need to have these systems in place, but I think the amount of money spent on some of them has to be put in perspective and related to what’s the real threat out there. We have major issues like guns in the hands of children, drunk driving, drug abuse, etc., that do massive damage to our country’s population year after year.

**Cheryl Gauthier:** Since 2001 most discussions have focused on the failures in biodetection; however, there have been many success stories. It’s time to move forward and promote progress by recognizing what has been accomplished in various locations throughout America. It is also time to engage all of the stakeholders in this effort to bring about a national capability which, in the end, will itself deter bioterrorism.

**Author Contributions:** All authors confirmed they have contributed to the intellectual content of this paper and have met the following 3 requirements: (a) significant contributions to the conception and design, acquisition of data, or analysis and interpretation of data; (b) drafting or revising the article for intellectual content; and (c) final approval of the published article.

**Authors’ Disclosures of Potential Conflicts of Interest:** Upon manuscript submission, all authors completed the Disclosures of Potential Conflict of Interest form. Potential conflicts of interest:

- **Employment or Leadership:** T. O’Brien, Tetracore.
- **Consultant or Advisory Role:** None declared.
- **Stock Ownership:** M. Hollis, Innovative Biosensors, Inc.
- **Honoraria:** None declared.
- **Research Funding:** M. Hollis, Innovative Biosensors, Inc.
- **Expert Testimony:** None declared.

**Role of Sponsor:** The funding organizations played no role in the design of study, choice of enrolled patients, review and interpretation of data, or preparation or approval of manuscript.

Previously published online at DOI: 10.1373/clinchem.2009.139493