COMMENTARY

Building an Integrated Enterprise: Increasing the Efficiency and Effectiveness of CBRNE Detection and Response

By Rick "Ozzie" Nelson and Rob Wise

December 6, 2012

In the midst of a constrained fiscal environment, the United States and the entities designated to protect it face difficult questions regarding how to best prepare for security incidents that may be viewed as relatively unlikely or low probability yet could have potentially devastating consequences, most notably the use of chemical, biological, radiological, nuclear, or high-explosive (CBRNE) weapons on American soil. Although the probability of terrorists using simpler means—such as mass shootings—to strike the United States appears much higher, the potential impact of a successful CBRNE attack demands that the nation prepare for this threat.

Though they may require comparatively more time and skill to build or acquire than conventional weapons, the proportional effects of CBRNE weapons are significantly greater. The "Amerithrax" attacks of 2001, for example, involved only a small amount of anthrax yet succeeded in paralyzing portions of the U.S. government. Furthermore, the danger of terrorists and others acquiring and potentially utilizing these weapons is not likely to decrease in the near future. Groups such as al Qaeda in the Arabian Peninsula (AQAP) continue to pursue CBRNE weapons as a means to strike the United States, as evidenced by their recent attempts to produce the toxic chemical ricin.[1] The rapid spread of technology, including emerging technologies such as 3-D printing, will likely only make the development of such weapons simpler, allowing nonstate actors to acquire CBRNE capabilities that were previously available only to nation-states. Further, instability in nations that possess CBRNE weapons, such as Syria, raises the risk of existing stockpiles falling into dangerous hands.[2] Faced with these threats, the United States has little choice but to work to defend itself against CBRNE weapons.

The United States has developed a robust series of measures intended to counter CBRNE weapons at multiple points before they reach U.S. shores. However, no matter the effectiveness of these efforts, the possibility remains that a device could evade detection or even be manufactured within the United States itself. As such, domestic efforts designed to detect and respond to a CBRNE incident are a critical component of the nation's security, representing the last and perhaps most vital line of defense against these weapons.

Over the past decade, the United States has worked to strengthen its ability to detect and respond to CBRNE threats, building a significant architecture spanning federal, state, and local governments. This has led to a myriad of offices, systems, and programs tasked with addressing various elements of the threat. For example, the Department of Homeland Security (DHS) houses biological detection programs, yet the Department of Health and Human Services is responsible for medical preparedness for biological attacks, while the Department of Defense controls many of the personnel and resources that would be deployed in the event of a biological incident, including the National Guard Weapons of Mass Destruction Civil Support Team (WMD CST). In addition to these federal entities, first responders at the state and local level are a vital component of CBRNE detection and response efforts; these individuals serve not only to maintain CBRNE expertise at the local level, but would likely be the first to arrive at a CBRNE event. Due to efforts at all levels of government, significant resources can be brought to bear to detect and respond to CBRNE

[1] Eric Schmitt and Thom Shanker, "Qaeda Trying to Harness Toxin for Bombs, U.S. Officials Fear," *New York Times*, August 12, 2011, http://www.nytimes.com/2011/08/13/world/middleeast/13terror.html?pagewanted=all.

[2] Sarah Sorcher, "Deadly Uncertainty: The Reason Syria's Chemical Weapons Are So Dangerous," *Atlantic*, July 16, 2012, http://www.theatlantic.com/international/archive/2012/07/deadly-uncertainty-the-reason-syrias-chemical-weapons-are-so-dangerous/259850/.

events. However, a variety of questions remain as to whether the current architecture is properly aligned to maximize CBRNE detection and response capabilities, especially as budgets are tightened and spending reduced. If the United States is to be as secure as possible against the threat of CBRNE weapons, efforts to increase effectiveness and efficiency must be explored.

Challenges to Efficiency and Effectiveness

Although the United States has succeeded in building a number of individual offices, program, and capabilities designed to detect and respond to CBRNE events, there are a variety of challenges that continue to hamper the effectiveness of counter-CBRNE efforts. First among these is simply the difficulties presented by the multitude of various entities working on these issues within the federal government. Responsibility for various elements of CBRNE detection and response is spread across numerous executive agencies rather than housed under a single entity, an architecture that demands close coordination and cooperation across departments. Furthermore, this distributed architecture can make the implementation of common, government-wide policy difficult.

This challenge extends not only to agencies, but even to specific offices within those agencies. For instance, DHS alone maintains two separate offices involved in CBRNE detection: the Domestic Nuclear Detection Office (DNDO) and the Office of Health Affairs (OHA). These offices, though they share the ultimate mission of countering CBRNE threats, work independently of one another and administer two separate detection systems. Furthermore, neither is operational, instead relying on entities such as U.S. Customs and Border Protection for implementation of their detection programs. Recently, the House Appropriations Committee highlighted the potential for unnecessary duplication and confusion under such a system and called into question the benefits of such diffusion.[3] Whether or not the committee's recommendation to consolidate DNDO and OHA is warranted, the distributed architecture of CBRNE detection and response does present a variety of inherent challenges to efficiency and effectiveness.

While working across numerous federal agencies may pose difficulties, the necessity of coordination with state and local first responders presents a host of additional challenges. Federal agencies may have the specialized resources and expertise most appropriate for meeting a CBRNE threat, but it is ultimately state and local entities that are most likely to first detect or respond to a CBRNE incident. This dynamic demands that state and local first responders are not only able to quickly communicate detailed CBRNE-related information to federal agencies, but that they know how to recognize and react to CBRNE threats. In addition to the technological challenges of such communication, many first responders lack the security clearances necessary to access the classified information that might assist them in preparing for a CBRNE event. While cooperation between federal and state and local entities is essential, there remains significant room for improvement in this regard.

At the most basic level, there are a host of challenges posed by the fundamental differences between the various threats that comprise "CBRNE," as well as between the cultural and organizational dynamics of the communities involved in countering these weapons. Among the key differences between individual CBRNE threats are the distinct consequences their impact would yield. These weapons have the potential to impair citizens and resources in different ways, requiring a distinct response capability for a host of potential events. Furthermore, nuclear material and weapons have traditionally been the preserve of the federal government, while biological threats have been the domain of the medical community, and chemical threats largely the concern of private industry. Each of these communities brings with it different priorities; for instance, the U.S. government's primary concern in the face of a CBRNE attack may be the larger strategic situation, while the medical community may worry most about public health. This can easily contribute to differences in prioritization of resources and hamper coordinated effort. Additionally, these communities each operate according to different timetables; the government following the demands of the fiscal year, while the medical community and private industry operate within longer or shorter timeframes determined by their own internal dynamics. Products of a threat that cuts across multiple disciplines, these differences can generate an element of friction, as well as a lack of focus and cohesion in counter-CBRNE efforts.

[3] "Department of Homeland Security Appropriations Bill, 2013: Consolidation of Weapons of Mass Destruction Defense Programs," H.R. 112-492 (2012), http://thomas.loc.gov/cgi-bin/cpquery/?&sid=cp112d60yh&r_n =hr492.112&dbname=cp112&&sel=TOC_41924&.

Finally, given that CBRNE detection and response is inherently a technology-intensive venture, there are numerous challenges associated with research and development. The decentralized nature of CBRNE efforts has led to an equally decentralized system to develop associated technologies, in which multiple departments and offices may be conducting research and development of which others are entirely unaware. This not only limits the ability of these entities to work together to build better technologies, but it may in fact lead to outright duplication of efforts. Furthermore, in recent years government research and development has invested heavily in basic research. Although there is certainly value in basic research, it has proven extremely costly, and its direct application to the development of new technologies has, at times, been limited. Technology holds the potential to dramatically improve CBRNE-related efforts, but necessary advances will likely prove elusive if these research and development challenges are not overcome.

Progress through Integration

Taken as a whole, these myriad challenges present a significant barrier to improving the efficiency and effectiveness of CBRNE detection and response efforts. Some have suggested that a consolidation of offices, programs, and capabilities would serve to address many of these issues. However, rather than focusing on reorganizing specific offices, the path forward may instead lie with the closer integration of various components within the CBRNE detection and response enterprise. By focusing on integration, there is a possibility of increasing the effectiveness of the disparate efforts across federal, state, and local governments. Furthermore, integration holds the potential to improve efficiency as well. For instance, greater integration might reduce duplicate efforts undertaken by different agencies and could serve to better streamline research and development programs. These gains in efficiency are especially important in the present budget environment, as funds for homeland security are cut. If the agencies responsible for CBRNE detection and response are to continue to fulfill their missions with fewer dollars, taking measures to optimize their efficiency will be necessary.

Recognizing the value of integration, the various components of the CBRNE detection and response enterprise have already begun taking steps to build closer ties. The Biodefense Leadership Group, established in January 2012, is a noteworthy attempt to better align OHA and DHS's Science and Technology (S&T) Directorate, while S&T has also begun to work through the First Responder Group (FRG) in order to better gauge and attempt to meet the technological needs of the first responder community.[4] Such efforts hold great potential, yet additional steps toward integration will likely be necessary if efficiency and effectiveness are to be maximized.

Potential additional measures to increase both the tactical and strategic integration of the CBRNE detection and response enterprise must focus on both policy and technology. Given that DHS S&T is already beginning to move toward greater integration, the continued streamlining of CBRNE-related research and development is a natural next step. Due to budget cuts, the enterprise can no longer afford a multitude of independent research and development programs. In order reduce redundancy and increase efficiency, research and development efforts within DHS, and possibly across the CBRNE detection and response enterprise, should be unified under, or at the very least coordinated through, a centralized office such as S&T. In addition to cutting costs, centralizing research and development may have the added effect of increasing the compatibility of new technologies with one another, further increasing integration.

At the same time, the federal government needs to coordinate more closely with private industry in order to reduce research and development costs. While government entities like S&T may once have been able to devote significant funds to basic research, they must now employ their limited dollars more strategically. Greater integration and cooperation between government and industry will allow them to jointly identify late-stage technology where additional government funds would lead to viable, useful products that could quickly be fielded. By leveraging industry, the CBRNE detection and response enterprise has the opportunity to realize significant savings while continuing to improve technological capabilities.

[4] Department of Homeland Security (DHS), "Science and Technology Directorate Support to the Homeland Security Enterprise and First Responders," http://www.dhs.gov/st-frg.

As the CBRNE detection and response enterprise and industry work to develop these new technologies, they must continue to keep integration, as well as real-world, multirole utility in mind. Ultimately, much of the technology developed will be destined for and utilized by the first responder community. As such, any new products being deployed will need to be designed to fit naturally into the daily activities of those who will be expected to use them. A complaint often heard from first responders is that while CBRNE detection and response equipment provided by the federal government may serve its specific purpose well, it is so unlikely to be employed that it almost never continues to be trained with or carried after it is acquired. As such, dual or multiuse technologies that provide first responders additional utility in their day-to-day activities, rather than additional burdens, should be prioritized. Developing such technologies and understanding how they can best be integrated into the first responder community will require additional coordination among federal, state, and local entities.

Perhaps the most important function new research and development can fulfill is to increase information sharing, and thus integration, between the disparate entities involved in CBRNE detection and response. If counter-CBRNE efforts are to be optimized, a common information-sharing architecture across the various entities involved, as well as integrated supporting technology, will likely be required. The National Information Exchange Model (NIEM) has been suggested by some as such a potential architecture. While NIEM should be adopted, its critics, citing concerns of scalability and complexity, may prevent it from being implemented. Whether NIEM is adopted or not, a common architecture for sharing information would greatly improve integration and therefore effectiveness. However, in addition to a common architecture, common technological systems are needed. As new technologies are explored, of greatest value will be those that are portable, can interface and share data with other systems, and can quickly and easily present complex, specific data in a comprehensible manner, such as through geospatial displays. The full value of integration will only be realized if it is supported by a common framework and technologies for the sharing of vital information.

However, even if common systems are put in place, information sharing, and thus integration, is unlikely to succeed if those on the front lines are not able to access the information being shared. As such, there is a need to explore methods of lowering classification barriers for first responders. This may involve granting a greater number of security clearances to state and local first responders or, if this is infeasible, possibly establishing a system to more readily allow first responders to be read on and read off CBRNE-related documents. However, in order for these barriers to be lowered, the first responder community will need to advocate forcefully for greater access to information. An integrated approach to CBRNE detection and response is predicated upon the rapid sharing of information, making classification barriers a significant hindrance in efforts to combat the CBRNE threat.

Beginning the process of integration may at first appear daunting, yet there are a number of factors that could serve to assist in easing this transition. Given the current fiscal situation, the cost of such integration will be a significant concern for many. Although the initial steps toward integration will certainly require additional resources, the process will almost certainly serve as a cost-cutting measure in the long term. Furthermore, there are existing examples of integration from which to draw tangible lessons, as well as a natural point at which to begin. The Integrated Chemical, Biological, Radiological, Nuclear, and Explosive (ICBRNE) pilot program, begun in 2009, served to bring together DHS S&T, the Los Angeles first responder community, and private industry to design and test a hand-held, off-the-shelf system that could relay live CBRNE-related information between first responders and experts.[5] Many of the lessons learned from this program, about the importance of collaboration and the types of technologies needed, can provide useful insights as the CBRNE detection and response enterprise moves toward integration. Additionally, there is an opportunity to begin quickly applying these lessons in the field as DHS expands the Securing the Cities (STC) nuclear detection program from New York City to Los Angeles and Long Beach.[6] The STC program, intended to build the regional capacity of local first responders to detect nuclear materials, represents a perfect testing ground for implementation of new efforts at integration. Given these factors, the path toward integration becomes significantly less challenging.

---

[5] Elaine Pittman, "Los Angeles County Prepares for a Nuclear Explosion," *Government Technology*, November 17, 2010, http://www.govtech.com/public-safety/Los-Angeles-County-Nuclear-Explosion.html.

[6] DHS, "DHS Announces the Expansion of the Securing the Cities Program to Los Angeles/Long Beach Area," press release, October 15, 2012, http://www.hsdl.org/?view&did=723935.

Ultimately, there is no consolidated, single architecture that would perfectly address the multitude of challenges associated with CBRNE detection and response. Although there may be potential benefits to various methods of consolidation, each would also necessarily require sacrifices, given the diversity of disciplines involved. However, the various offices, programs, and capabilities currently spread across federal, state, and local governments can and should be integrated to a greater degree. Such integration can begin to be developed through a variety of efforts, including the streamlining of research and development, greater engagement of private industry, a focus on fielding integrated, multifunctional technologies for first responders, the adoption of an information-sharing architecture and supporting technologies, and the lowering of classification barriers. Through integration, there exists an opportunity to forge a more efficient and effective CBRNE detection and response enterprise and strengthen our nation's security against these devastating weapons.

Rick "Ozzie" Nelson is director of the Homeland Security and Counterterrorism Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C. Rob Wise is a research assistant with the CSIS Homeland Security and Counterterrorism Program.