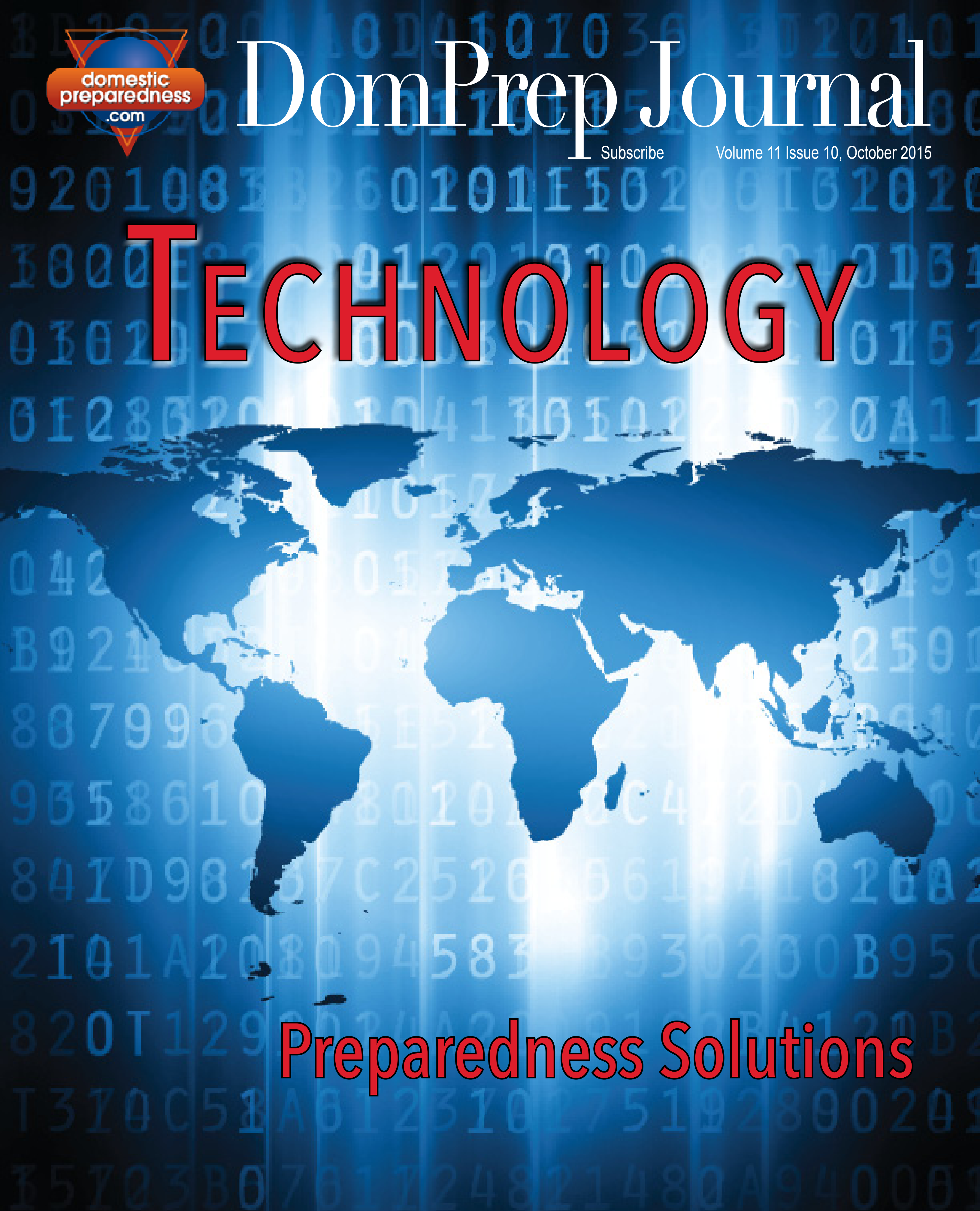
domestic preparedness .com

DomPrep Journal

Subscribe

Volume 11 Issue 10, October 2015



TECHNOLOGY

Preparedness Solutions

Since 1998, Integrating Professional Communities of Homeland Security, Preparedness, Response & Recovery

4th Annual

NATIONAL HEALTHCARE COALITION PREPAREDNESS CONFERENCE

Ensuring Readiness, Building Resilience

December 1-4, 2015

Sheraton San Diego Hotel & Marina - San Diego, California

The **Annual National Healthcare Coalition Preparedness Conference** brings together professionals in the fields of healthcare, public health, emergency medical services and emergency management nationwide to share best practices and learn about coalition activities in our communities. This year's event will showcase training models, plans, tools, and other resources that promote effective coalition work in preparedness and response. The conference will be co-sponsored with the Veterans Emergency Management Evaluation Center (VEMEC) of the U.S. Department of Veterans Affairs and in conjunction with the California Association of Health Facilities.

from CONCEPT to PRACTICE
VEMEC
Veterans Emergency Management Evaluation Center

CAHF
disaster preparedness program dpp

For more information, please visit NHCRC's website: healthcarecoalitions.org

Contact us at info@healthcarecoalitions.org.

Business Office
517 Benfield Road, Suite 303
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Staff

Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

James D. Hessman
Editor Emeritus

Catherine Feinman
Editor
cfeinman@domprep.com

Kimberly Arsenault
Project Manager
karsenault@domprep.com

Carole Parker
Manager, Integrated Media
cparker@domprep.com

John Morton
Senior Strategic Advisor
jmorton@domprep.com

DomPrep Journal is electronically delivered by the IMR Group Inc., P.O. Box 810, Severna Park, MD 21146, USA; phone: 410-518-6900; email: subscriber@domprep.com; also available at www.DomPrep.com

Articles are written by professional practitioners in homeland security, domestic preparedness, and related fields. Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher. Text is the opinion of the author; publisher holds no liability for their use or interpretation.

Featured in This Issue

About the Cover: Technology enables communities around the world to communicate, share information/data, conduct research, train, and perform many other routine and extraordinary tasks. However, although technology enhances daily operations, there is no substitute for good planning, training, and preparedness. (Source: ©iStock.com/traffic_analyzer)

Editorial Remarks

By Catherine Feinman

Technology involves a combination of tools, techniques, and procedures that people use to perform tasks. In emergency and disaster planning, these critical tasks help to build more resilient communities by improving the safety and security of their members. In this issue of the *DomPrep Journal*, subject matter experts address real-world problems with science-based solutions, which include equipment, training, and facilities that provide flexibility, accessibility, security, and even cost effectiveness.

Rachel Bartholomew and Richard Ozanich lead this issue with a discussion on how scientists and researchers at Pacific Northwest National Laboratory are helping with the development of new technologies for detecting, sampling, and studying various contaminants and unknown substances using a scientific-based approach.

In addition to hand-held and drive-through technology, infrastructure can be designed "smarter," as described by Jessica Brown and Allan Swan. Disaster response scenarios require flexibility, speed, and security, which may include temporary structures that meet pharmacy and biosafety facility needs yet are designed to be portable and affordable.

Technology alone is not the solution, though. Learning how to use new tools, equipment, and other resources, of course, requires training. Solid planning and training, as emphasized by Steven Bucci, must accompany any technological changes. In rural Idaho, for example, Darin Letzring has helped emergency planners and public health professionals learn how to leverage information tools and navigate vast resources available online.

Similarly, Dawn Thomas describes how virtual training techniques can expand the training ground and reduce costs. Although technology facilitates information sharing, there also is an ongoing debate over information security and privacy protection. Ellen Cornelius addresses this issue, citing examples such as protecting patients' electronic healthcare records.

Rounding out the issue, Roddy Moscoso addresses another ongoing debate, which involves community-police relations. By leveraging technology – including body-worn cameras, gunshot detection, and social media monitoring – perhaps some of these relationship gaps can be repaired and visual perceptions and communication can be improved. Having the right tools ensures that emergency personnel can perform their critical tasks at every stage of an emergency or disaster.

Technology Development & Science-Based Solutions

By Rachel Bartholomew & Richard Ozanich

Science-based research is useful in analyzing and reducing risks through the development of new technologies for detecting, sampling, and studying various contaminants and unknown substances. Teams of scientists at Pacific Northwest National Laboratory play a large role in ensuring that first responders have the necessary tools to perform their critical tasks.

Pacific Northwest National Laboratory (PNNL) is involved in many research activities related to domestic preparedness, emergency response, and recovery from manmade or natural adverse events. The laboratory's scientists and engineers focus on delivering practical, science-based solutions to important problems. One of PNNL's major strengths is the ability to integrate research across various disciplines at the laboratory and bring them to the market, where first responders and emergency managers can put them to work.

A few examples illustrating PNNL's diverse work in preparedness, response, and recovery are detailed below. These examples range from developing risk analysis and reduction tools and visual sampling plans for the support of confident decision-making during events, to innovative approaches to improving chemical and biological sample screening and detection, such as the development of smartphone microscopes for biological detection and ultra-trace explosives vapor detection systems.

Risk Analysis & Reduction Tools

In the field of operations research (OR), sometimes called "the Science of Better," scientists employ techniques like mathematical programming, event simulation, and decision science to tackle some of the complex challenges facing the world. PNNL's OR team is staffed with world leaders in relevant technical fields and works closely with sponsors and other stakeholders to present concrete, usable solutions, as well as the analysis needed to influence policy decisions across the national-security and emergency-response spectrum.

For example, working with law enforcement and the emergency management community, PNNL has developed a Risk Reduction and Resource Assessment Model (3RAM) for the Washington State Ferries system. This tool automatically determines the best deployment of security measures and limited tactical security assets using an adaptive, risk-based approach. 3RAM has been used to counter the threat of vehicle-borne improvised explosive devices in various operational environments since 2011. PNNL has also developed and is currently incorporating active-shooter and other threats into 3RAM's capabilities.

PNNL has also developed the cutting-edge Physical and Cyber Risk Analysis Tool (PACRAT) software to analyze vulnerability and risk. This software tool blends assessment processes

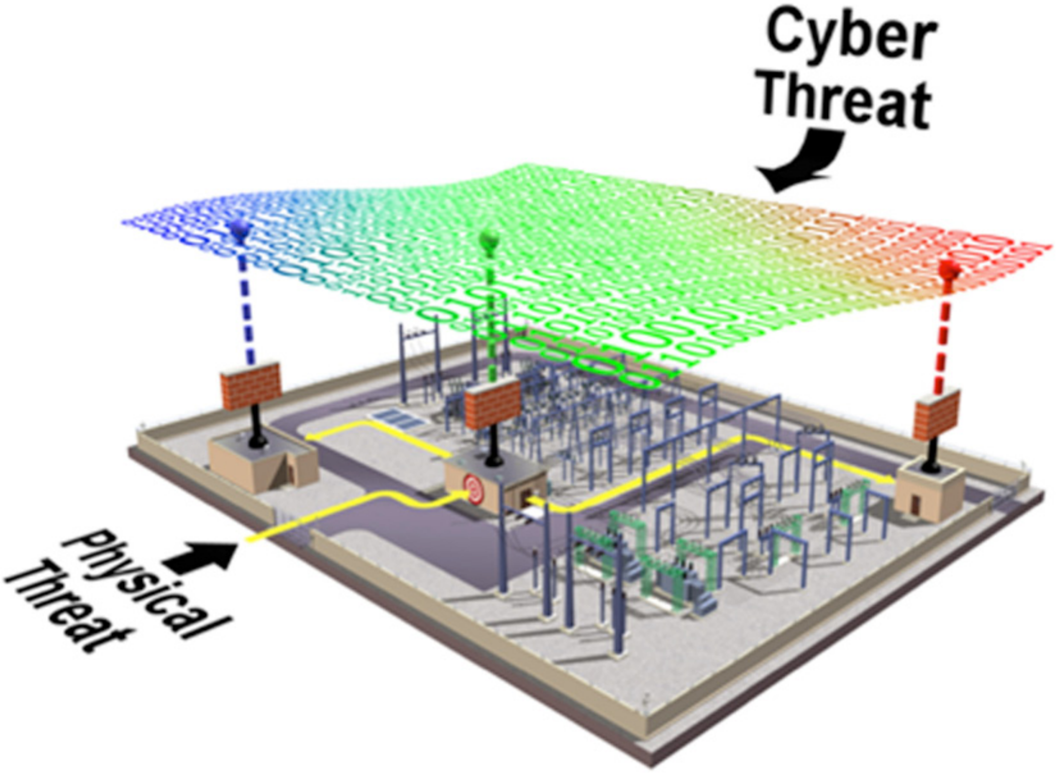


Fig. 1. The PNNL PACRAT Vulnerability and Risk Analysis Software Platform models the interdependent nature of cyber and physical threats.

used in both physical and cyber security domains to provide a comprehensive evaluation of a proposed security strategy, taking into account interactions and interdependencies between cyber and physical systems.

Additionally, in work for the Department of Homeland Security's Domestic Nuclear Detection Office, PNNL has developed and deployed the Radiological and Nuclear Risk Assessment Methods (RNRAM), an integrated terrorist risk assessment tool that helps decision makers craft optimal detection-system and law-enforcement strategies within the Global Nuclear Detection Architecture. The RNRAM models radiological and nuclear threats and helps analysts assess them. RNRAM can also assist in determining the effectiveness of nuclear detection systems and concepts of operations to counter these threats. Because of its flexible structure, this tool can be adapted for application to other threat spaces by other agencies.

Visual Sample Plan (VSP)

If a large outdoor area or building were to become contaminated with harmful material, samples would have to be collected and analyzed to assess the extent of contamination right after the event, as well as to monitor the effectiveness of cleanup after decontamination. However, selecting the optimal sample collection locations to support response decisions is a challenge. PNNL's VSP is a freely available statistical sampling design software tool that couples site, building, and sample location visualization capabilities with optimal sampling design and statistical analysis strategies. VSP helps ensure that the right type, quality, and quantity of data are gathered to support confident decisions and to provide statistical evaluations of the data with decision recommendations.

VSP was developed with support from the Department of Energy, the Environmental Protection Agency, the Department of Defense, the Nuclear Regulatory Commission, the Department of Homeland Security, the Centers for Disease Control and Prevention, and the United Kingdom, and has more than 5,000 users worldwide. The tool has been used to support sampling in contexts such as environmental remediation, soil characterization, groundwater monitoring, unexploded ordnance sites, and facility decommissioning.

The underlying statistical methodology used by VSP allows real-time evaluation of the tradeoffs between increased confidence in decisions and costs or number of samples required. Designed for the nonstatistician, VSP uses plain language and a user-friendly interface to elicit inputs for the underlying statistical methods. All equations used and assumptions made are documented in an automatically generated report along with maps, plots, and diagnostic graphics.

Site maps and building plans can be drawn or imported into VSP and used to identify and visualize where samples should be located. Map background imagery and 3D visualization of buildings and furniture models provide an intuitive view of sampling across a site or facility. VSP helps users obtain answers to the following questions:

- How many samples do I need?
- Where should I take samples?
- What decisions do my data support?
- How confident am I in those decisions?

Smartphone Microscope

Janine Hutchison and Rebecca Erikson at PNNL have led the development of a smartphone microscope (SPM) for analysis of both biological samples and unknown powders. Because smartphones are robust, everywhere, and easy-to-use, they provide an ideal platform for tools to differentiate potential biothreats like *Bacillus anthracis* (anthrax) from commonly encountered hoax powders. A 3D-printed clip holds a spherical lens that quickly slides over the camera of a smartphone, providing 350× magnification at a cost of a few cents. At this magnification, objects 1/50th the diameter of a human hair are readily observable. Further features under development include improved image resolution and automated image analysis to meet the needs of end users. Commercial smartphone camera applications allow easy control of focus, exposure time, and other camera settings. The SPM platform is ideal for

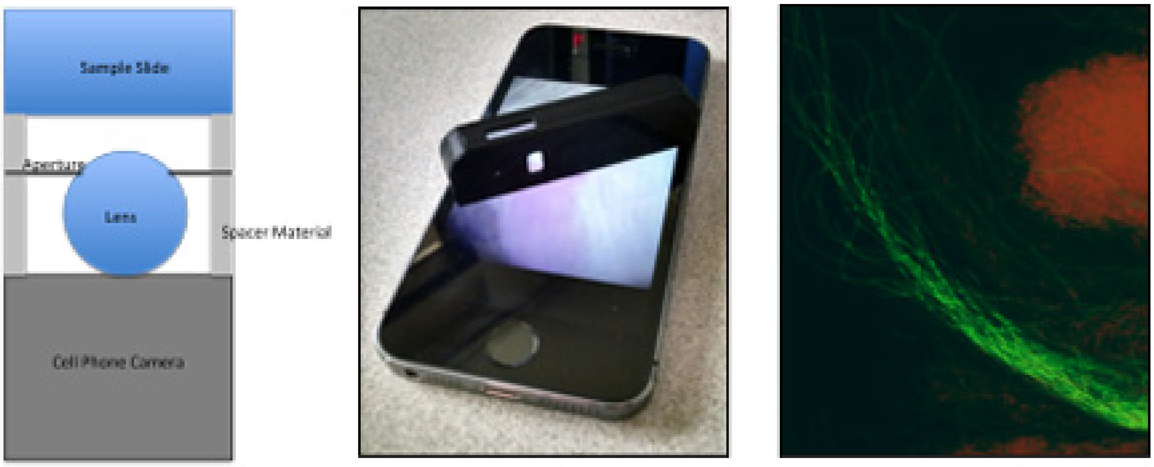


Fig. 2. Left: A schematic illustration of PNNL's smartphone microscope (SPM) with a sample slide. Center: An actual SPM, which is compatible with Android and Apple smartphones. Right: Fluorescence image from an SPM of stained Bacillus anthracis Sterne vegetative cells that have germinated from spores. Viable cells are stained green and dead (non-viable) have been stained red.

rapidly transmitting images and data out of a "hot" zone to reach decision makers or to obtain technical support from a subject matter expert.

Beyond microscopy and imaging, the SPM can also incorporate field chemical and biological detection and analysis capabilities using low-cost optical filters and advanced fluorescence and energy-absorbance technologies. These user-friendly advances open opportunities to replace cumbersome and costly optical readers currently used in the field.

Ultra-Sensitive Explosives Vapor Detection

Robert Ewing and his team at PNNL have developed a new approach to explosives vapor detection that is thousands of times more sensitive than current technology and provides results in less than 5 seconds. For the first time, real-time detection of parts-per-quadrillion levels of explosive vapors is possible without preconcentration. This technique provides a noncontact method for detecting explosives that is less invasive and covers a larger sampling area compared to contact swipe-sampling techniques.

Vapors of explosive compounds such as RDX and PETN are at low parts-per-trillion levels at room temperature. Because of dilution of vapors in the environment, detection levels below parts-per-trillion are required. To achieve parts-per-quadrillion sensitivity, PNNL developed an atmospheric flow tube-mass spectrometer (AFT-MS). This instrument provides unprecedented sensitivity in detecting a broad range of explosives including nitroglycerine, RDX, PETN, tetryl, and various formulations such as plastic explosives, blasting gels, and several types of gunpowder. Using a simple preconcentration device, the AFT-MS could perform ultra-trace detection (sub-parts-per-quadrillion) to detect RDX vapor within a cargo container in less than 5 minutes.

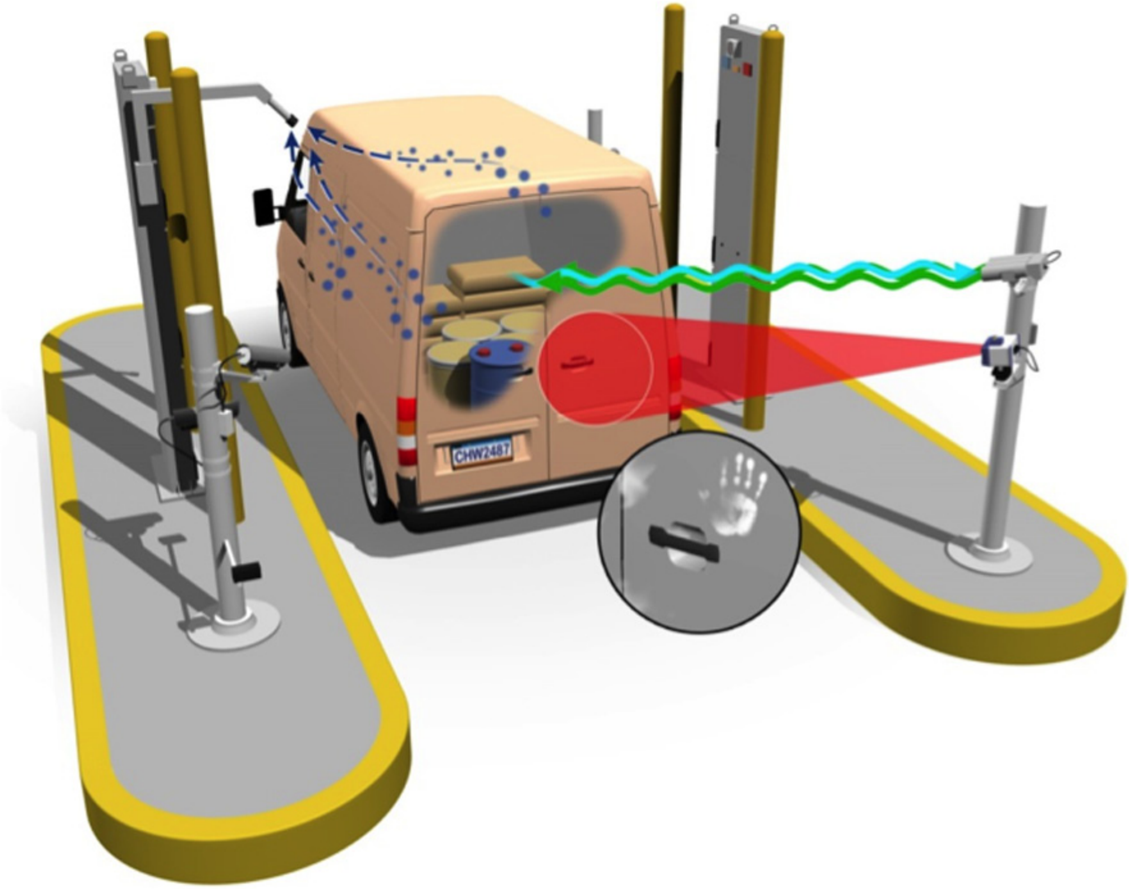


Fig. 3. Illustration of the possible use of the AFT-MS technology in combination with other rapid screening technologies for detection of various types of threats in a drive-through portal.

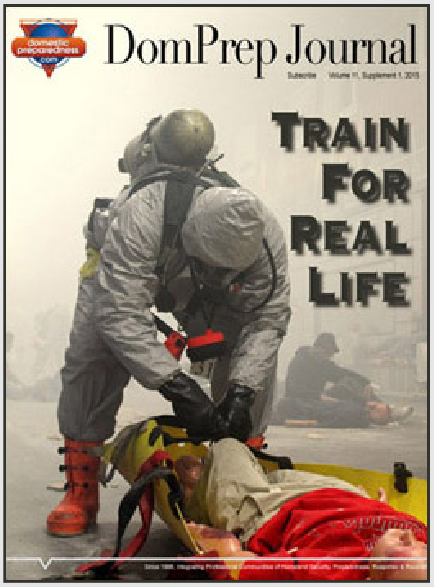
Interdisciplinary teams at PNNL address many of America's most pressing issues in energy, the environment, and national security through advances in basic and applied science. Founded in 1965, PNNL employs 4,300 staff and has an annual budget of about $950 million. It is managed by Battelle for the U.S. Department of Energy's Office of Science. As the single largest supporter of basic physical science research in the United States, the Office of Science is working to address some of the most pressing challenges facing the nation today.

For additional information on:
Pacific Northwest National Laboratory, visit http://www.pnnl.gov
Physical and Cyber Risk Analysis Tool (PACRAT), view http://www.youtube.com/watch?v=Hh5NEpJZGZw
Visual Sample Plan (VSP), visit http://vsp.pnnl.gov
Smartphone microscope (SPM), visit http://1.usa.gov/1VO4mtx

Rachel A. Bartholomew (pictured), Ph.D., is a senior research scientist at Pacific Northwest National Laboratory and has over 15 years of experience in molecular biology, including developing and testing systems for environmental biodetection, cell culture and diagnostics, and national security applications. She has publications in the area of biodetection, cell culture, and molecular biology, including an upcoming chapter on polymerase chain reaction (PCR) in the American Society of Microbiology's publication "Methods in Environmental Microbiology" (4th edition). She received an undergraduate degree in biology from Case Western Reserve University and a Ph.D. in physiology from Cornell University.

Richard M. Ozanich, Ph.D., has worked in the biodetection field for over 20 years. He is a subject matter expert in biodetection and optical spectroscopy and has a broad base of knowledge in the fields of chemistry, biology, and measurement instrumentation. He is currently working on evaluation and testing of biothreat detection instruments and assays to improve the selection and use of field biodetection equipment for first responders. His research includes development of automated fluidics instrumentation and microparticle-based methods for sample preparation and rapid detection of biothreats. He is active in the area of bioresponse and development of standards and best practices and is a member of ASTM International (American Society for Testing and Materials) Committee E54 on Homeland Security Applications. He received a B.S. degree in chemistry from the University of Washington and a Ph.D. in analytical chemistry from the University of Washington.

Significant contribution to this article was made by Cynthia J. Bruckner-Lea, Ph.D., who is a senior scientist and program manager at Pacific Northwest National Laboratory. She is a recognized biodetection expert with over 30 years of experience in the development and application of biological detection systems for environmental monitoring, medical, and national security applications. She is an American Association for the Advancement of Science Engineering Section Fellow, and she has served on several National Academy of Science Committees conducting studies related to chemical and biological detection. She has over 50 publications and 10 patents. She received a B.S. degree in chemical engineering from the University of California, Davis, and a Ph.D. in bioengineering from the University of Utah.



In June 2015, DomPrep was invited to take an exclusive inside look at the Center for Domestic Preparedness, a training facility that offers something beneficial to all of DomPrep's readers. After spending a week in Anniston, Alabama, DomPrep's Kimberly Arsenault and Catherine Feinman compiled this comprehensive supplement with text, photos, and podcasts of the experience they had at the training facility.

Technology vs. Good Planning & Training

By Steven P. Bucci

There is no single solution to cybersecurity concerns. Technology is advancing, but nothing can replace solid planning and training. All three pillars are necessary to balance cyberthreats. If too much emphasis is placed on one pillar, the vulnerability gap will expand. Ensuring the constant growth and evolution of this trilogy is currently the best way to thwart threats that are ever evolving.

Americans habitually look for a technological fix (a "silver bullet") that will solve whatever problem arises, which includes cybersecurity concerns. Although cybersecurity is the ultimate in high-tech issues, a perfect technological solution does not currently exist. So, technology cannot simply replace good planning and training.

If technology is not a panacea, then something else needs to be done to provide adequate cybersecurity for organizations, families, and individuals. It is fundamentally necessary to provide training and invest time and energy in emergency or crisis management planning in order to mitigate current risks. Neither aspect is terribly expensive, but finding the time and resources to plan and train can be inconvenient. Without training, all the technological investments in the world will not provide adequate protection, and systems will be vulnerable.

Future Solutions & Current Training

This is not to say that there will never be a viable solution. The government and particularly the private sector are currently investing huge amounts of research capital in efforts to find that silver bullet. For example, in the past 10 years, IBM Corporation has spent almost $2 billion on research and development related to security. If the silver bullet – whatever that may turn out to be – can be "attached" to a network, or run on machines, it would allow operations in the cyber domain to be free from hacking, cyberattacks, and data theft (be it identities or intellectual property).

The value of such a discovery would be astronomical, but it has not yet been found; and it is not likely to be found in the short term. In the absence of perfect protection, a proactive approach to emergency or crisis management is necessary and involves three critical parts: (a) train personnel; (b) plan well to achieve a level of resilience that allows organizational functions to go forward despite an attack; and (c) maximize the best, less-than-perfect technology solutions available, updating with great regularity and sufficient frequency.

Looking at the seminal Mandiant Intelligence Center Report ("APT1: Exposing One of China's Cyber Espionage Units") on Chinese government hacking, it is clear that, although the Chinese are very sophisticated, their most consistent entry point to hacked networks has been old-school social engineering. A well-constructed spear-phishing attack has been

China's primary method. To thwart such attacks, personnel must be trained beyond the infantile, compliance-driven, online drivel that passes for annual training in many cases.

Training must be rigorous, dynamic, and relevant to job responsibilities. Without that and without the management staff participating, the message is clear: security training is not important. A highly trained workforce will not stop all cyberintrusions, but it will stop a lot more than an untrained workforce could prevent. This is the foundation.

Vital Questions & Viable Solutions

Next, the highest levels in the organization must realistically plan, asking vital questions, which include:

- How will we react when (and not if) we are attacked?
- Do we have backups?
- How will we shift duties to fix the problem and continue executing our missions?
- Who is in charge should a breach occur?

These questions and more should not be decided upon after an information technology infrastructure has been attacked. Investments in planning before an attack result in much better decisions and actions when needed, which greatly increases the overall resilience of the organization.

Once the "human" factors of training and planning are addressed, it is time to invest in the best technological protection that fits the company's organizational model and budget. Again, this may not prevent an attack, but it will stop many who wish to do harm. There is a greater return on security investments when equipped with a trained workforce and a good remediation plan than with only protective devices and software on the network as a defense strategy. With solid research and good counsel, investments in technology would reflect a continual process that facilitates the evolution of protective assets as the threat environment changes.

The bottom line is simple. Investments in technology alone do not sufficiently protect networks and remove the need for good training and dynamic, insightful planning. In today's highly competitive cyber arena, a myriad of potential enemies are targeting security gaps. Without all three pillars – planning, training, and technology – an organization is extremely vulnerable. This vulnerability is unnecessary and unacceptable.

Steven P. Bucci, Ph.D., former Green Beret, is director of the Allison Center for Foreign Policy Studies at The Heritage Foundation. He also is an adjunct professor of leadership at George Mason University and an associate professor of terrorism studies and cyber security policy at Long Island University. He serves on the advisory board of the MIT Geospatial Data Center and is an advisor to the Prince of Wales/Prince Edward Fellowship program at MIT and Harvard. He previously served as a lead consultant to IBM on cyber security policy and as a special forces commander in the U.S. Army, where he assumed the duties of military assistant to Defense Secretary Donald H. Rumsfeld. After retiring from the Army in 2005, he served as deputy assistant secretary of defense for homeland defense and defense support to civil authorities at the Pentagon, and was the primary civilian overseer of U.S. Northern Command.

The Continuing Battle Over Privacy vs. Security

By Ellen C. Cornelius

In this electronic age, there is a constant struggle between sharing critical information and protecting individual privacy with adequate security to prevent data and documents from falling into the wrong hands. To address these concerns, expectations of privacy, knowledge of liabilities, and development of policies must be examined.

Some people might argue that there is virtually no privacy left as the Internet, government, and media dramatically affect daily routines. Others would say that, although daily life is not as private as it once was, privacy is a worthy sacrifice in order to defend against hackers and terrorists. The battle for a clear winner continues to rage, while several questions remain:

- How do expectations of privacy change based on security concerns?
- Who is liable in the aftermath of data breaches and identity theft?
- Are there policy solutions that could help balance these concerns?

Expectations of Privacy

The expectation of privacy is deeply rooted in legal tradition and culture. For example, published in 1890, "The Right to Privacy," was a seminal article by Samuel Warren and Louis Brandeis (later a Supreme Court Justice) that still resonates today. Against the backdrop of the invention of the camera and the coverage of upper class society in the gossip pages of local newspapers, Warren and Brandeis' article in the *Harvard Law Review* explained the right of the individual citizen to be left alone. They started first with principles. The U.S. Constitution provides the right to life, liberty, and property. Property law protects the tangible, such as land and personal possessions, as well as the intangible, such as trade secrets and trademarks. Warren and Brandeis asserted that the right to privacy emerges from the right to life and liberty.

The right to privacy does not prohibit publication of material that is in the public or general interest. However, common law – or norms embodied in judicial decisions – protects an individual from being compelled to express his or her thoughts, sentiments, or emotions, except on the witness stand. The individual retains the power to limit publicity but, as soon as the individual decides to publish information, the right to privacy with respect to that particular piece of information is waived. If a person limits publicity, but a reporter uses a camera to take pictures surreptitiously, then the only applicable law is torts or, in this case, a lawsuit claiming invasion of privacy. Warren and Brandeis argued that the courts should protect the right to be left alone – that is, one's right to privacy.

Expectations of privacy change depending on security concerns. For example, closed-circuit television (CCTV) has attracted attention from privacy advocates who argue that they should be able to travel discreetly, without the government's knowledge. With CCTV, facial recognition software, and international databases, a person can be tracked on every continent around the world. Abuses by law enforcement and computer errors can be difficult to identify and correct. However, many of these fears have been addressed by cities in laws that regulate or limit how visual footage may be used by the government.

Beyond government interests, the general public takes photos and videos constantly. In a sense, individuals surveil each other. Facebook has perhaps the largest facial recognition database in the world. National level and local level law enforcement are heavily invested in facial recognition databases and software as well. In 2005, the identities of terrorists in London were discovered in a few weeks after they attacked three underground stations and a double-decker bus. In 2013, the terrorists who attacked the Boston Marathon were identified within a few days. Boston, Massachusetts, had only 55 law enforcement cameras in 2007 and the number has grown. Facial recognition software has made searching footage much faster.

Security advocates might say that observing possible terrorists and criminals makes communities more secure. They support increasing the number of cameras and license plate readers and argue that cameras with features like high definition, the ability to zoom in, and automated movement to focus on gunshots provide law enforcement with important opportunities to prevent and solve crimes. In response, policies to mitigate the impact of this technology focus on who can view the footage, how it can be used, and how long the recording will be kept.

Breaches, Thefts & Liabilities

Data breach, identity theft, and corporate liability are of great concern. In June 2014, over 1 million CareFirst BlueCross BlueShield subscribers had their personal data stolen. The first class-action lawsuit alleges negligence, breach of contract, and violations of Washington, D.C.'s consumer protection and data-breach notification statutes.

The Anthem breach announced in February 2015 was even bigger. Payment data was transmitted through the BlueCard network, but the data was being retained in an unencrypted fashion. It involved 80 million subscribers and has spawned more than 50 class-action lawsuits. Claims include violations of the Health Insurance Portability and Accountability Act (HIPAA) and state laws. However, data breach and identity theft are not just risks for insurance companies or healthcare systems. Many employers, big or small, maintain employees' names, addresses, social security numbers for tax purposes, and bank account information for payroll. There are at least three different ways that businesses can be liable for data breaches: HIPAA regulatory liability; negligence; and state statutory liability.

Medical identity theft can be used to falsify medical history, get surgeries, obtain or sell prescription drugs, and blackmail. Electronic medical records can be sold illegally for about $50 each, whereas cyber thieves may only earn $1 for social security numbers. Under HIPAA, any organization that handles patient information under a "business associates agreement" with a HIPAA-covered entity is equally liable for breaches as the covered entity itself, in accordance with the law. The courts often rely on HIPAA's privacy and security rules as the standard of care in negligence cases. Other best practices that the courts rely on include: encryption, monitoring of business associates, mitigation of risks, and increased accountability.

The U.S. Department of Health and Human Services (HHS) recommends administrative, physical, and technical safeguards to protect patient information:

- *Administrative safeguards* include security management processes, security personnel, information access management, training and management, and evaluation.
- *Physical safeguards* include facility access and control as well as workstation and device security. A HIPAA-covered entity must: limit physical access to its facilities while ensuring that authorized access is allowed; implement policies and procedures to specify proper use of and access to workstations and electronic media; and have policies and procedures regarding the transfer, removal, disposal, and reuse of electronic media to ensure appropriate protection of electronic protected health information.
- *Technical safeguards* include access control, audit control, integrity control, and transmission security.

Businesses may be liable for civil penalties if the courts determine that they are negligent in protecting electronic health records. According to the U.S. Department of Health and Human Services, about 75 percent of health records are electronic, and healthcare providers use mobile devices to store, process, and transmit patient information. If a mobile device is hacked, then the healthcare provider or business associate may face penalties. In July 2015, the National Institute of Standards and Technology, National Cybersecurity Center of Excellence, issued a "How to Guide," which provides a sample solution for protecting electronic health records on mobile devices. The guide uses commercially available products to more securely share electronic health records. A court may use this as the standard of care and apply it in negligence cases.

Four elements are required to establish a case of negligence: duty, breach, causation, and damages. Reasonable care speaks to duty. Principal factors to consider in ascertaining whether the person's conduct lacks reasonable care include: (a) the foreseeable likelihood that this conduct will result in harm; (b) the foreseeable severity of any harm that may ensue; and (c) the burden of precautions to eliminate or reduce the risk of harm (see Restatement [Third] of Torts: Liability for Physical Harm § 3 [P.F.D. No. 1, 2005]). Negligent conduct may consist of either an act, or an omission to act when there is a duty to do so (see Restatement [Second] of Torts § 282 [1965]).

Businesses have a duty to safeguard customer information. For example, Maryland's Social Security Number Privacy Act requires employers to transmit social security numbers over the Internet with a secure connection or encryption. Businesses should know what personal information the organization has on its computers, then secure that information physically, with passwords, or with assigned identification numbers that are different from the social security numbers.

Many companies spend a significant amount of money on antivirus products and firewalls, but hackers can breach such perimeters. What companies really need are detection products that stop an attack once the system has been breached. Hiring and training also are important. Organizations should train employees on the data security plan, as well as on protocols so employees can spot, report, and remedy potential security threats. Background checks on employees who have access to personally identifiable information are also important, while confidentiality agreements can be used to address security with contractors.

Liability can also ensue from a violation of a state statute. For example, the Maryland Personal Information Protection Act requires an employer to maintain reasonable security procedures and practices for personal information. Consumers must receive notice of a data breach, and the notice must include:

- A description of the information compromised;
- Contact information for the business, including a toll-free number if the business has one;
- Toll-free numbers and addresses for Equifax, Experian, and TransUnion;
- Toll-free numbers, addresses, and websites for the Federal Trade Commission and the Office of the Attorney General of Maryland; and
- A statement that the individual can obtain information from these sources regarding steps to avoid identity theft.

Policy Solutions to Address Concerns

There are also policy developments in cybersecurity to consider. For example, in the healthcare industry, the development of a unique patient identifier is under consideration. Currently, medical record numbers are not unique and not transferable. Another policy proposal is that businesses create business continuity plans, so they can continue to operate if the organization's data were catastrophically breached.

The federal Cybersecurity Information Sharing Act of 2015 (S.754) has been proposed to promote the sharing of cyberthreat information among government agencies and private sector businesses. As drafted, S.754 would offer incentives to the private sector to share information about cyberthreats with the government. Supporters, including senators from both parties and many in the private sector, say the information sharing legislation would create stronger defenses against hackers. However, privacy advocates are concerned about the bill's treatment of sensitive information, arguing that it would violate the right to privacy. Moreover, security experts have questioned whether the bill would be effective.

Against this complicated backdrop, policy makers continue to try to balance privacy and security. Privacy advocates push back against the use of technology to monitor threats and favor tighter regulations, whereas security advocates push for a more widespread use of technology and the development of threat-detection tools. Undoubtedly, there are many challenging calls to be made in the year ahead.

Ellen C. Cornelius, J.D., is senior law and policy analyst at the University of Maryland Center for Health and Homeland Security (CHHS) and an adjunct professor at the University of Maryland Francis King Carey School of Law, where she teaches a course entitled Law and Policy of Cybersecurity. Her article, "Chinese Hackers and their New Target – Federal Employees," was published in the 2014. Through CHHS, she has been detailed to the District of Columbia (D.C.) Homeland Security and Emergency Management Agency since 2008. She has drafted a variety of plans for D.C., including the Emergency Shelter Plan. In 2013, she became the liaison to D.C.'s public-private institution – the Business Emergency Management Operations Center.

Rural Idaho – Research Tools & Training Exercises

By Darin Letzring

Although there is no shortage of information, the quality and validity of information varies considerably. Learning how to identify effective information tools and use them to their full potential takes time. However, in rural Idaho, information-gathering skills are being taught to help emergency planners and public health professionals to better navigate the vast World Wide Web of information.

Exercises and disasters are always better explained and better understood with 20/20 hindsight vision. After-action reviews provide such hindsight as they monitor and evaluate activities. Equipped with this information and other shared lessons learned and best practices, planners have the ability to influence the way their communities respond to future disasters and ultimately improve the ability to respond more effectively. However, a key question is, "What information is worth adopting and where do we get it from?"

In the era of the World Wide Web of information, it is easy to be overwhelmed by the sheer volume of data and resources, making it difficult to discern relevant information from background noise. Teasing out the nuggets of valuable information can often be challenging without an organized approach. Erin Strange, emergency preparedness coordinator at Bear Lake Memorial Hospital in Montpelier, Idaho, commented, "One of the biggest challenges in emergency preparedness is simply finding resources [and the] tools to get to reliable information."

Two Training Periods With One Focused Objective

The information-gathering approach has to be strategic and focused in order to provide the maximum reward. To this end, emergency planners from throughout southeastern Idaho gathered twice for three-hour training periods to learn how to gather scientific, evidence-based information for emergency planning and response. When combined with regular after-action reports from events, evidence-based data provides a solid foundation for mitigation and response measures. A significant result of this training is the increased opportunities for these rural emergency planners to access additional information via the Internet from their desks in rural Idaho.

In order to collect the appropriate data, the information-gathering process must leverage existing and accessible resources. Southeastern Idaho Public Health collaborated with the Idaho State University (ISU) Health Sciences Library to provide information-gathering training for emergency planners from the regional healthcare coalition. Subject matter expertise for the training, which was funded by a one-year grant from the National Library of Medicine (NLM), included: Dr. Ruiling Guo, who was a health sciences librarian/associate professor at ISU Health Sciences Library at the time of the grant and now teaches at the Health Care Administration Program in the Division of Health Sciences at ISU; and Rhonda D'Amico, who was the healthcare liaison for Southeastern Idaho Public Health and is now the health district's program manager for Statewide Healthcare Innovation Plan (SHIP).

For this particular training, the project focused on emergency planners in the region's rural, critical-access hospitals, but the training was offered to healthcare professionals from all agencies within the healthcare coalition and private sector in the region. Project goals included:

- Creating a needs assessment;
- Developing and conducting a training program to directly address the results of the needs assessment; and
- Developing new partnerships between emergency planners and library professionals.

"As with any best practice, information gathering requires a systematic approach guided by the actual needs that the data and resources should address."

Before the training, all of the emergencyplannerssurveyedhadan interest in learning "how to search for disaster health information effectively and efficiently for emergency preparedness and disaster response." The pre- and post-tests showed that there was a statistically significant increase in knowledge and skills in information searching after training. Participants learned more about and increased their confidence in using NLM's information resources.

Finding & Using the Right Information Tools

As with any best practice, information gathering requires a systematic approach guided by the actual needs that the data and resources should address. In the ISU Health Sciences training session, the approach included:

- Awareness of NLM resources and basic disaster health information searching;
- The development of search strategies;
- An introduction to PubMed, Disaster Lit, and other selected disaster health information resources; and
- Understanding of how to evaluate online disaster health information and how to access and request full-text articles.

Rural Hospitals. *Source:* ©iStock.com/Ulrich Knaupe

Participants were given case scenarios to search for evidence in PubMed, Disaster Lit, and other related online resources. The training ended with the introduction to disaster and emergency management decision-making tools, such as WISER, CHEMM, and REMM.

In addition to course material, participants received three hardcopy books: (a) an in-depth resource about healthcare preparedness and response; (b) a basic primer to anyone new to healthcare preparedness; and (c) a workbook to assist in planning. Finally, attendees received several pocket information guides that could be added to their "go kits." The training materials are available on the project website. In the future, the training presentations will be available on TRAIN, a public health industry learning management system.

This exercise in conducting information gathering illustrates the importance of an organized, systematic approach that is focused and covers a broad range of resources because the volume of resources is large and not always appropriate, accurate, or up-to-date. For these reasons, partnering with existing institutions to help train and strategically focus information gathering can save a lot of time and be a valuable investment for mitigating, preparing for, responding to, and recovering from future disasters.

Darin Letzring is the program manager for Public Health Emergency Preparedness at Southeastern Idaho Public Health, where he was previously the all-hazards planner with a total of ten years in the program. He also serves as an emergency preparedness liaison officer in the U.S. Marine Corps Reserves. An advocate for rural America, he has served on various working groups within the National Association of County and City Health Officials (NACCHO).

JOIN US!

63rd IAEM Annual Conference & EMEX

Expanding the Spectrum of Emergency Management

November 13–18, 2015

PARIS HOTEL • CLARK COUNTY, NV

http://iaemconference.info/2015/

Virtual Exercises – A Cost-Effective Option

By Dawn Thomas

Some exercises require a hands-on environment, whereas others can thrive in a virtual training space. FUSION X is one federally sponsored exercise that has evolved from a tabletop event at a single location to a virtual training for participants, who require flexibility and cost-effectiveness, at various locations throughout the United States.

Those responsible for their organization's preparedness efforts have often been told that they must find ways to do more with less. With budgets tightening even further, exercises are a likely victim of this trend, as large exercises can be extremely costly to sponsors. However, with continuing and increasing threats associated with natural incidents, industrial accidents, and deliberate acts, members of the homeland security enterprise need the opportunity to practice their skills in meaningful ways. For those supporting preparedness at the local, state, regional, tribal, and federal levels, this means considering new possibilities for exercising targeted audiences using less expensive methods, but without sacrificing value.

Exercising Fusion Centers

On 2 August 2012, the Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) sponsored FUSION X, a timely one-day exercise that allowed eight fusion centers to share information and analysis across their National Network of Fusion Centers (National Network) partners. Over the preceding years, DHS had invested a great deal of time and money to support the development of individual fusion center capabilities, including the publication of fusion center guidelines and baseline operational standards. By 2012, internal capabilities grew, and DHS I&A determined that the next logical step was to begin testing information receiving, gathering, analysis, and dissemination across the National Network. Their exercise design included elements of both a tabletop and a functional exercise, with players sitting at different tables and receiving injects that drove interaction.

Exercise support personnel occupied a simulation cell and provided pieces of the puzzle as the scenario advanced. Additionally, each table had a facilitator and an evaluator, who recorded exercise play and developed an after-action report for each table. After the exercise, the lead evaluator gathered and aggregated all exercise data, and developed an after-action report for the National Network. Although DHS I&A and the participants considered the exercise a success – and important strengths and areas for improvement were identified – the cost (both in time and money) was not insignificant. Analysts were away from their desks for two to three days, and a large support staff was needed to facilitate and record the exercise.

In 2014, DHS I&A embarked on an effort to conduct the second exercise in the FUSION X series, using the same tabletop concept as the one used in 2012. As the planning process proceeded, issues of funding and level of effort put the project on hold, and the exercise was postponed. With a continued belief in the value of simultaneously exercising multiple members of the National Network, the newly formed DHS I&A Continuity and Exercise Programs Branch and their exercise planning team began developing a new version of FUSION X – a functional exercise that would take place in a completely virtual, yet secure, environment.

Moving to a Virtual Training Ground

The exercise, conducted in July 2015, covered a large geographic footprint, but with no travel required. Players were located in fusion centers in Arizona, Colorado, Idaho, New Mexico, Utah, and Wyoming, in addition to DHS Watch and Warning Center in Washington, DC. Continuity and Exercise Programs Branch leadership and members of the exercise support team (composed of an exercise director, simulation cell staff, and evaluators) were also spread out, participating from Washington, Virginia, Texas, New Mexico, and Washington, DC.

Although the exercise support team provided training, fusion centers were responsible for providing their own facilitators and evaluators. The former were responsible for: (a) supporting scenario development; (b) injecting their pieces of the Master Scenario Events List; and (c) leading discussion at their respective locations. The latter were responsible for: (a) documenting exercise play; (b) gathering participant feedback forms; and (c) providing their analysis of events through exercise evaluation guides. In addition to making observations on the execution of the fusion centers' critical operational capabilities, the exercise support team also collected and aggregated reflections on the design, conduct, and evaluation of a virtual exercise, including the following:

- The virtual exercise allowed analysts to better mimic their day-to-day roles and responsibilities by more accurately replicating their work environments. The injects – in the form of social media posts, situation reports, and memos from the various intelligence community partners – reflected the information received during a typical workday, and participants were able to respond authentically. Moreover, with a growing effort to gather, analyze, and share information gained through social media and other electronic methods, the virtual environment provided an excellent background for demonstrating fusion center capabilities.
- FUSION X 2015 was less expensive to execute and demanded less time from exercise planners and players than an exercise where participants come together at a single location. Although the Continuity and Exercise Programs Branch made an initial investment in developing an exercise that could be successfully executed in the virtual environment, planners at the national and fusion center levels avoided travel costs, hours lost to travel, and an investment in backfill. Moving forward, the exercise can now be repeated with other groups of fusion centers with minimal time, effort, and investment.
- The exercise planning team had excellent coordination with fusion center planners, using Homeland Security Information Network (HSIN) Connect to host the traditional Homeland Security Exercise and Evaluation Program (HSEEP) planning processes and to share all exercise documents with the planning team. However, players needed much more direction on exercise "rules of engagement." Uncertainty about when to engage each other versus when to engage the simulation cell slowed the pace of play during the first few hours of the exercise.

- Players practiced, or were introduced to, virtual tools of their trade. During FUSION X 2015, players used HSIN's situational awareness platform (SitAware) as one of their methods of communication. Although not all fusion centers had used SitAware in the past, they recognized during the course of the exercise its value for sharing information during fast-paced incidents.

The execution of FUSION X 2015 provided valuable insight into not only how fusion centers can more efficiently exercise their analysts, but also how virtual exercises might be used to serve a wider homeland security audience. In looking toward other applications of virtual exercises, organizations should ask the following three questions when determining whether a virtual exercise might be appropriate for them:

- "Does how we want to exercise translate into a virtual world?" Although many organizations have made good use of virtual training for tactical procedures – for example, hazardous materials, active shooter response – virtual exercises may be less appropriate for these operations. A virtual exercise does not allow responders to practice hands-on operations, such as donning and doffing personal protective equipment, practicing technical processes such as sampling, or exercising the use of equipment that is paramount to their operations.
- "Does what we want to exercise translate to a virtual world?" For those considering an exercise based on a capability such as operational coordination or public information and warning, a virtual exercise might prove effective. Organizations can place players in the virtual chairs like the ones they occupy in the real world, which encourages information sharing via the mechanisms they use each day. Social media, which is part of the daily information-gathering practices of many emergency responders and receivers, can be seamlessly integrated into the Master Scenario Events List of a virtual exercise.
- "Does the scope of our intended exercise translate to the virtual world?" The scope of some exercises allows for easy and effective virtual play, providing more realism than a tabletop exercise. For example, jurisdictions may want to exercise the critical first 30 minutes of a response, when people are not yet at their desks and are forced to share information and make decisions from wherever they are. Likewise, virtual prevention exercises – done in small increments over a long period of time – may allow players to exercise analytical tradecraft while still effectively performing their daily activities. Finally, exercises that include a large number of participants from different geographical locations may be a good fit for a virtual approach.

Virtual exercise will not be appropriate for all organizations or for all exercises. However, in an environment of limited budgets and extensive virtual communication, organizations should consider the value of shifting their exercise paradigm into the virtual world.

Dawn Thomas is an associate director of CNA's Safety and Security division, where she has been supporting homeland security planning, training, and exercises for 11 years. She holds a B.S. from Carnegie Mellon University, and an M.A. from The Hebrew University of Jerusalem.

Running to the Police, Not Away From Them

By Rodrigo (Roddy) Moscoso

Building sustainable communities is a long-term effort that includes reestablishing positive relationships between police departments and the communities they serve. Repairing these damaged relationships will mean changing the visual perception, improving communication, providing education, and building awareness for the community members.

Since the August 2014 riots in Ferguson, Missouri, following the police shooting death of Michael Brown, significant media attention has been placed on the public's perception of law enforcement officers and their use of force. Several cases captured on video – including the death of Eric Garner in New York City during a sidewalk arrest – have latched on to the narrative that the police have become, to some, a source of fear rather than protection, an enemy rather than an ally.

Broken Relationships

The April 2015 riots in Baltimore, Maryland, following the death of Freddie Gray while in police custody served as another stark example of the significant distrust that exists between law enforcement officers and portions of the community that they are charged to "protect and serve." Although the events that unfurled will be analyzed for years to come, the unfortunate reality for the city of Baltimore is that significant parts of its citizenry appear to have lost faith in the police; they do not look to them for help in times of crisis.

During the Baltimore protests, Mayor Stephanie Rawlings-Blake made the critical decision to order the police to "create a space" for the protestors, acknowledging later that doing so had also given "those who wished to destroy space to do that [as well]." However, when some unknown number of "bad actors" looted and set fire to their own neighborhoods within this space, the local population did not call out for assistance from the police gathered only blocks away. Worse, the police knew that they were not wanted. This broken relationship played out on live television, and became yet another example in a yearlong series of events highlighting a line between the police and the citizenry.

> ***"The number of arrests made and tickets issued are not necessarily measures of success," said David Mitchell, director of public safety and chief of police for the University of Maryland at College Park.***

In some areas, the "us vs. them" viewpoint has become "the norm," illustrating the modern relationship between police officers and the communities they serve. This fractured bond benefits neither the public nor the police and inevitably leads to further distrust and more-frequent instances of conflict and even violence. The questions now are how to better define the relationship and how to make it happen.

One Police Chief's Perspective

"In times of crisis, we want people to run to the police, not away from them," said David Mitchell, director of public safety and chief of police for the University of Maryland at College Park (UMD), in a personal interview on 16 June 2015. Mitchell, who has served in cabinet-level positions in Maryland and Delaware as state police superintendent and secretary of the Department of Safety and Homeland Security, respectively, believes that a culture shift in law enforcement – not more training – is what is needed to improve the relationship between the general public and the police.

He worries that law enforcement has "lost legitimacy" with the public. "Our business is to sell safety, and to do so we must redefine our success as, 'the creation of sustainable neighborhoods'," Mitchell added. He is also leery of what he sees as an overreliance (and focus) on crime data used internally by police departments to measure crime rates across distinct geographic areas.

"CompStat is often used by [police] executives to embarrass individuals, which does not necessarily achieve important public safety outcomes. It's a useful tool to be sure, but it is not able to measure our success in building positive relationships with our community," he said, adding that, "the number of arrests made and tickets issued are not necessarily measures of success."

Mitchell also believes that the manner in which the police respond to the community during incidents is equally important. These efforts include:

- *Visual perception* – "We don't dress in BDUs [battle dress uniforms], we use uniforms of the day," said Mitchell noting that BDUs do not necessarily present an "approachable presence" and may create a visual perception of force that is not conducive to building a positive relationship with the community.
- *Communication* – "Ongoing communication is also key to building trust," said Mitchell. The UMD Police Department uses multiple communications channels to keep the community informed of events, large and small, taking place in the area. "We use Nixle to send targeted, geo-fenced alerts to faculty and students not just about public safety related issues, but also to alert them of road closures, construction issues, etc.," he noted. Doing so establishes a "dialogue" that serves to open communication channels that "work both ways" and to encourage people to value and rely on the information coming from the police department.
- *Education* – The UMD police department educates students and faculty on how to respond collaboratively during a significant event, such as on-campus active

shooter. "We teach 'Run, Hide, Fight' to our community," said Mitchell. "It is critically important, and it gives our students and faculty a sense that we are working together during these types of situations," he added.

- *Awareness* – Training and communication also helps to avoid the potential confusion caused by a lack of awareness of who the police are, "We can't meet each other for the first time during a crisis," said Mitchell.
- *Documentation and review* – The UMD Police Department documents "every use-of-force incident," including when an officer only "pulls a gun," for later review and analysis. Mitchell noted that the department is currently reviewing its use-of-force training with "a new focus on de-escalation techniques."

Mitchell also believes that leveraging technology is another way to build trust. Examples include:

- *Body-worn cameras* – "We use body-worn cameras, and the officers love them," said Mitchell, noting that the technology creates an "objective observer" that both parties can acknowledge (and perhaps adjust their behavior to) during a police interaction.
- *Gunshot detection* – The UMD is in the process of installing "ShotSpotter" gunshot detection solution in and around campus, which will facilitate a more efficient and timely response to locations where gunshots have occurred.
- *Social media monitoring* – The UMD monitors social media proactively in order to identify incidents that may require a police response. "Social media allows us to establish a real-time dialogue with our community," said Mitchell. "We want them to tell us what is happening, that's why we are here," he added.

Long-Term Dividends

Building "sustainable communities" is a long-term effort and one that will require vigilance and a consistent effort by all community members, including the general public, businesses, government, and public safety. Rebuilding the trust between law enforcement and the public is a critical step in this process. "We 'sell' safety, and that means that we have to deliver it. And we will be more successful if the community sees us as a full partner in achieving safety," said Mitchell.

Following the events of the past year, this may be a "tough sell." Building trust is also not something that is ever accomplished quickly. However, small and incremental steps can reap dividends over the long term. Starting a dialogue, even one way, can be a good first step.

Rodrigo (Roddy) Moscoso currently serves as executive director of the Capital Wireless Information Net (CapWIN) Program at the University of Maryland, which provides software and mission-critical data access services to first responders in and across dozens of jurisdictions, disciplines, and levels of government. Formerly with IBM Business Consulting Services, he has more than 20 years of experience supporting large-scale implementation projects for information technology, and extensive experience in several related fields such as change management, business process reengineering, human resources, and communications.

FilmArray

Modular Solutions for Compounding Pharmacies & Biosafety Facilities

By Jessica Brown & Allan Swan

A decade after Hurricane Katrina devastated the Gulf Coast region, the effects of underprepared healthcare systems are still apparent. Nearly a year after the first case of Ebola was diagnosed on U.S. soil, the West African nations most affected by the disease remain burdened by insufficient infrastructure to properly isolate and treat patients on a large scale.

Recent disasters in the United States and abroad have illustrated the need for rapid deployment of personnel and facilities to augment challenged healthcare systems. The regulated complexities of modern medicine demand quality, efficient healthcare facilities in which safety is the highest priority. The flexibility, adaptability, and security needed during a disaster response are often incompatible with the stick-built structures of traditional healthcare systems. There is a need for high-quality, rapidly deployable facilities in two particular areas of healthcare – compounding pharmacies and advanced biosafety facilities.

Compounding Pharmacies

"Compounding" is the creation by a licensed pharmacist of custom prescription medications that meet a patient's individual needs. Examples of common compounding practices include adapting the form, ingredients, or dosage strength of a drug to accommodate allergies or peculiarities with a patient's condition. Up to three percent of prescriptions issued in the United States currently are for compounded medications. As personalized medicine grows, so will this total.

The popular image of the compounding pharmacy was tarnished by the October 2012 fungal meningitis outbreak that was traced to several lots of contaminated injectable steroids produced by the New England Compounding Center, setting in motion efforts to better regulate these types of pharmacies. Yet the demand for compounded medications and the pharmacies that make them grows with an aging population and the number of drug shortages fueled by the economics of the pharmaceutical industry.

Drugs that serve a limited population are often discontinued by manufacturers who profit from producing more in-demand drugs. Compounding pharmacies have been filling the associated supply gaps since their inception, which was largely based on the need for injectable drugs. In late 2012, the Food and Drug Administration (FDA) said that approximately 85 percent of the 118 drugs listed in short supply were injectables. High-profile shortages of intravenous fluids in recent years have also raised concern, as these are among the most commonly needed medications in disasters.

Drug shortages and the growth of personalized medicine have not only increased the demand for compounding pharmacies, but also their importance in continuity of care during disasters. Pharmaceutical management in disasters is complex. Unlike other healthcare emergency resources – such as evacuation aids and personal protective equipment – pharmaceuticals typically have relatively short shelf lives that inhibit the ability to maintain adequate stores for emergencies that last longer than 72 hours. As large manufacturers consolidate, there is less redundancy in the supply chain, disruption of which is an obvious threat in most types of disasters. Given these factors, compounding pharmacies have a clear role to play in disaster response, and should be part of local and national preparedness efforts.

Biosafety Facilities

Facilities in which healthcare or public health personnel work with potentially infectious microorganisms and other biological hazards are known as biosafety facilities. These facilities are designated as biosafety level (BSL) 1, 2, 3, or 4 based on the laboratory practices, facility construction, and safety equipment requirements corresponding to the risk level of the microbes to be handled. Microbes that require level 4 biosafety, like Ebola, have a high risk of aerosol transmission and cause diseases that are frequently fatal. BSL 4 microbes demand the most stringent laboratory practice and safety equipment standards, and a separate structure or isolated and restricted area of a building with a specific exhaust system.

Advanced biosafety facilities have extensive application in disasters with capabilities and safety standards that lend them to use for flash laboratory capacity, patient isolation and development and efficacy testing of vaccine and treatment candidates. The need for such facilities was easily seen in West Africa at the height of the 2014 Ebola outbreak. In a region that lacked quick laboratory testing and patient isolation capacity, domestic and international responders struggled to stop the spread of this highly infectious disease. Global health leaders have responded with a search for innovative solutions to thwart such obstacles in future outbreaks. In the fall of 2014, U.S. President Barack Obama challenged the U.S. Agency for International Development to find new tools to help with the crisis.

Required Attributes for Utility in Disaster Response

The work performed in sterile compounding pharmacies and biosafety facilities must meet the highest standards for safety, meaning that their construction is traditionally time-consuming, costly, and beholden to multiple regulatory authorities. None of this is ideal for a disaster response scenario, in which flexibility, speed, and security are critical.

- *Flexible integration with existing healthcare systems* – Healthcare systems operating in disasters need adaptable solutions to facility and equipment shortages in order to maximize agility and cost-effectiveness. Response resources must be quickly integrated into existing health systems with minimal disruption to ongoing operations. The optimal scenario is often a self-contained facility that does not rely on another structure for its utilities or ventilation but can be located in close physical proximity to existing healthcare facilities, with interoperable communications and equipment. As with responders who are trained to be self-sufficient, these facilities must be self-sustaining.
- *Flexibility of purpose* – In day-to-day operations, pharmaceutical manufacturers, including compounding pharmacies, need the ability to quickly change the type of product or production capacity to meet market demands. The same

is true in a natural disaster when pharmacists are responding to the specific, unpredictable medication needs of patients who likely need immediate replacement of prescriptions. Similarly, a biosafety facility deployed for use in a disaster may be needed for a variety of changing purposes, which means a standardized facility with internal configuration is ideal.

- *Safety and security* – A team of U.S. Public Health Service pharmacists charged with standing up a fully functional pharmacy to serve a 480-bed federal medical station hospital in Mississippi in the days following Hurricane Katrina cited the need for a secure, lockable space with adequate refrigeration as one of its greatest challenges. This situation highlights the need for a reliable, closed, and solid structure. Along with the similar security considerations, advanced biosafety facilities require sturdy construction to adequately contain pathogens and protect healthcare workers and patients.
- *Speed and longevity* – A rapid-onset disaster, from a tornado to an outbreak of a novel pathogen, demands a quick response. Depending on the nature of the emergency, compounding pharmacies and biosafety facilities could both be needed with just days of notice in order to ensure the health and safety of an affected population. In many cases, the organization deploying a facility asset does not know the longevity of need from the outset. It is important to have facilities that can remain in place for extended periods of time and endure harsh weather conditions, where applicable.

Flexible Modular Solutions

As modular construction has evolved into a mainstream building solution, many sectors with disaster preparedness responsibilities have explored its use in meeting emergency needs. The Modular Building Institute, an association of manufacturers and dealers of code-compliant relocatable buildings, argued in a 2011 article, "Due to the accelerated, factory-controlled modular construction process, there is simply no better means of providing fast, transitional shelter, schools and medical facilities in times of great need than relocatable buildings."

In addition to their widely publicized use for temporary housing, there are multiple examples of post-disaster use of modular facilities:

- Modular units were used as counseling centers in New York following the 9/11 terrorist attacks.
- After the 2011 Joplin tornadoes, nearly 24,000 square feet of modular space provided classrooms for local schools.
- Mobile kitchen and shower units have supported disaster relief workers, with portability and flexibility of the interior configuration.

Healthcare systems are turning to modular construction even for daily use. Modular units have been used to build on to operating rooms and physician offices, expand diagnostic imaging clinic and dialysis center capacity, and provide temporary emergency departments and pharmacies to avoid business interruption while permanent structures are under construction. Most significantly, the Ebola treatment facilities at Emory and the University of Nebraska Medical Center incorporated elements of modular design – separability and flexibility – to ensure that the presence of the treatment units would not disrupt other operations.

The greatest appeal of modular construction is one of the key features for disaster response: flexibility. Modular units range from functional construction blocks that can be fit into existing facility infrastructure to stand-alone structures or "pods." Pods are prefabricated boxes designed and built off-site that contain their own air handling and fire suppression systems. This makes them independent from any ductwork and other infrastructure associated with an existing building. The ability to "plug and play," or select particular elements of a manufacturer's offerings, allows for the construction of larger, even multi-story, facilities made up of multiple modules. In the fall of 2014, a modular building manufacturer erected a first-of-its-kind 52-bed assisted living and memory care facility in Bradenton, Florida, that was constructed of 40 modular units. The building was completed at least two months faster than a comparable stick-built facility and was the first of 14 such structures planned across the state.

The Ebola crisis in West Africa demonstrated the need for rapid deployment and redeployment of biosafety facilities in an infectious disease outbreak, opening a new door for modular construction in healthcare. In fall 2014, high-containment manufacturing pod facilities that were originally developed with Department of Defense funding for biological and pandemic threat preparedness were being repurposed for use as patient isolation units in response to the Ebola outbreak.

Key attributes for modular health response

In addition to the potential for meeting the flexibility, speed, and security requirements, several other factors make modular construction attractive for healthcare emergency response:

- Portability – A key element to the speed of deployment of modular facilities is their potential for easy transport because of standardized size and construction techniques. Some companies have further enhanced portability by selecting building platforms that lend themselves to international travel, such as standardized intermodal shipping containers.
- Manageable costs – Traditional pharmaceutical production facilities have been hindered by new regulatory requirements that call for features like unidirectional workflow as well as heating, ventilating, and air conditioning systems that are segregated for different production areas. Manufacturers have touted modular facilities as a cost-effective solution for replacing outdated facilities while acquiring added benefits of flexibility.
- Localization – Another issue that has made modular construction an attractive option, in particular for drug manufacturers, is the ability to quickly stand up a facility that allows for local production. An interview with Paul Black, chief executive officer of Winston Medical Center, Louisville, Mississippi, on 17 June

2014 provides one example. After a tornado rendered the only hospital in Winston County, Mississippi, uninhabitable in April 2014, its administrators and state health authorities opted to use modular facilities, some provided commercially and others leant from other state emergency management authorities, to serve as temporary replacements for more than a year. The facilities included a trailer with a laminar flow hood for use as a compounding pharmacy. The quick acquisition of these assets allowed local healthcare staff to return to work quickly, heading off concerns about a repeat scenario of Hurricane Katrina, when many healthcare providers left the Mississippi Delta region in order to maintain their livelihoods since their places of work were slow to be replaced.

Remaining Challenges & Opportunities

The use of modular facilities in disaster response is not a new concept, and the perception of their utility is bound to negative stereotypes. In the aftermath of Hurricane Katrina, the Federal Emergency Management Administration trailers provided as temporary shelter to thousands exemplified the sluggish recovery of the housing sector and painful insurance claim processes. Structures that appear by nature to be temporary raise questions about whether they can possibly provide the same standard of safety and care as a stick-built permanent building. Yet the opportunity to provide focused, point-of-need, customized, quality healthcare faster, better, and cheaper are evident.

Perhaps the greatest challenge facing the use of modular facilities for compounding pharmacies for disaster response scenarios, particularly within the United States, is the same challenge that continues to complicate their day-to-day use. Although the FDA has authority to regulate drug manufacturing, compounding falls into the gap between state and federal oversight. This regulatory gap continues to evolve and, while some states' boards of pharmacy and emergency planners have acknowledged and made arrangements for use of mobile facilities in emergencies, others have not. Policy makers have the opportunity to support better healthcare in the aftermath of disasters by ensuring modular facilities can be deployed without unnecessary complications.

Jessica Brown (pictured), M.A., is a freelance writer with years of experience in healthcare emergency preparedness, including positions at the MESH Coalition, the Northwest Healthcare Response Network, and the Department of Defense's Center for Excellence in Disaster Management and Humanitarian Assistance. Previously, she was a reporter and editor at newspapers in Washington, Montana, and Virginia. She holds an M.A. in diplomacy and military studies from Hawai'i Pacific University and a B.A. in journalism and history from the University of Montana. She resides in the Seattle, Washington, area.

Allan Swan is a graduate student in health administration at Indiana University and interned with the MESH Coalition during the summer of 2015. The MESH Coalition (www.meshcoalition.org) is a nonprofit, public-private coalition that enables healthcare organizations in central Indiana to respond effectively to emergencies and remain viable through recovery.

Biologics Modular (BM) LLC provided MESH an unrestricted educational grant to develop this article. BM is a biomanufacturing company based in Brownsburg, Indiana, the company was formed in 2009. www.biologicsmodular.com

Dose Rate
0.055
FLIR