domestic preparedness .com

DomPrep Journal

Subscribe

Volume 14, Issue 3, March 2018

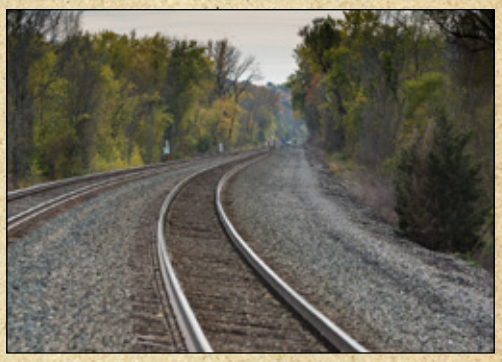
Roles in Disaster – Completing the Chain
By Catherine L. Feinman

Emerging Threats to Rail Infrastructure: Part II, Passenger
By Catherine L. Feinman

Podcast: Protecting Food, Air, and Water: Environmental Health
Moderated By Andrew Roszak

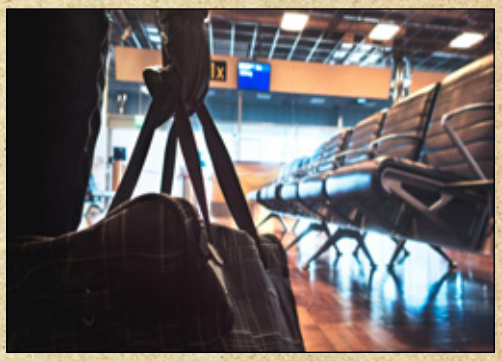
User Guide for Responder-Driven Technology Development
By Ann Lesperance & Richard Ozanich

The Key to Saving Lives in CBRNE Events
By Bobby Baker



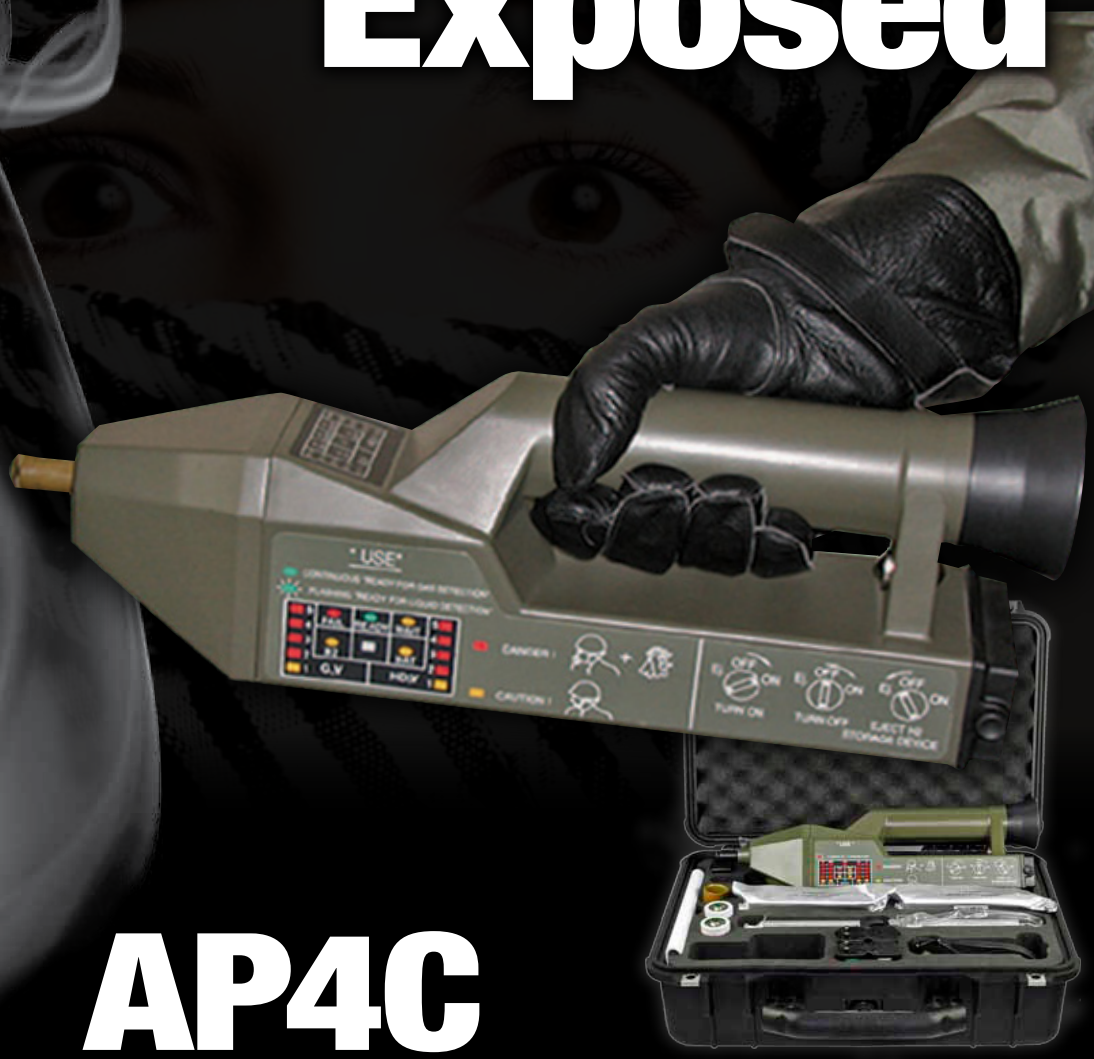
Rail Threats & Interdependencies – Thoughts for Discussion
By Rick Mathews

Podcast: MPAs & Disasters
Moderated By Andrew Roszak



Historical Argument for Hardening Facilities
By Michael E. Gray

Invisible Threats Exposed



AP4C

Portable Chemical Detection System
Protects First Responders, Military & Infrastructure

- Fast, Reliable Analysis of Invisible Hazards Saves Time & Lives
- Unlimited Simultaneous Detection Exposes Unknown Agents
- Low Maintenance & Operation Costs Save Money
- Rugged Handheld Design is Easy-To-Use With Minimal Training
- Complete System Includes Accessories & Case for Easy Transport

Learn More Online

PROENGIN

Chemical and Biological Detection Systems

Business Office
P.O. Box 810
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Staff
Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

Catherine Feinman
Editor-in-Chief
cfeinman@domprep.com

Carole Parker
Manager, Integrated Media
cparker@domprep.com

Advertisers in This Issue:

BioFire Defense

FLIR Systems Inc.

PROENGIN Inc.

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.

IMR GROUP

Featured in This Issue

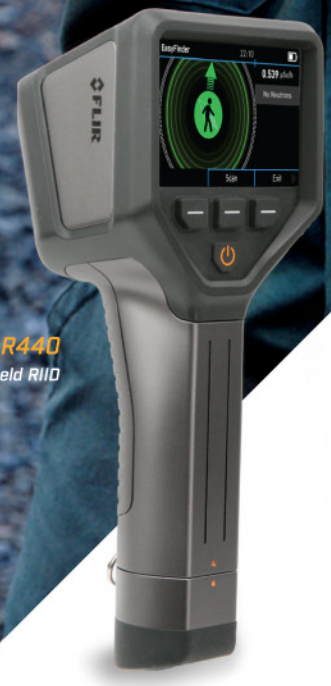
Pictured on the Cover: (top row) Feinman, Source: ©iStock.com/patpitchaya; Feinman, Source: DomPrep, 2018; (second row) Roszak, Source: ©iStock.com/amanalang; Lesperance & Ozanich, Source: PNNL, 2018; (third row) Baker, Source: ©iStock.com/Keith Nesbit; Mathews, Source: Mathews, 2018; (bottom row) Roszak, Source: iStock.com/YourNikonMan; Gray, Source: ©iStock.com/Tero Vesalainen

WE STEPPED UP SO YOU CAN STEP BACK.

The new FLIR identiFINDER® R440 lets you scan for radiological threats from farther away to keep you and your community safe.

The new R440 is a lightweight, sourceless RIID that can be operated with one hand and is IP67-rated to survive tough missions. Not only does the 2x2 NaI detector deliver sensitive and fast detection, but it also provides accurate identification during secondary screening. The new 360° EasyFinder™ Mode expedites decision-making to keep you safe.

Learn more at flir.com/R440



FLIR identiFINDER R440
Highly Sensitive, Sourceless Handheld RIID

FLIR®

Roles in Disaster – Completing the Chain

By Catherine L. Feinman

A passenger train derails in an urban community. Whether caused by intentional or unintentional factors, this incident would have consequences that go well beyond the rail company and the passengers traveling in these fated rail cars. Surrounding companies and communities would be affected, hazardous materials may be a threat, critical infrastructure beyond transportation could be impacted, cyber and physical security could be at risk, and so on. Mitigating these risks, threats, and vulnerabilities requires education, tools, and a desire to play a key role in disaster preparedness and response.

Rail incidents could affect all local stakeholders, so bringing them to the table to discuss potential threats as well as the roles and responsibilities that each stakeholder plays is critical. It all begins with education. For example, college students must decide which educational tracks they would like to follow based on the future jobs they would like to secure. Although similar, one or two words in a professional title could make a big difference when preparing for or responding to a disaster – for example, environmental health versus public health professions; or Master's of Public Administration (MPA) versus Master's of Business Administration (MBA). Lessons learned from previous incidents could provide critical information for decision makers, such as arguments for investing in more resilient plans, procedures, and structures.

Once they understand the various roles and define their own functions and responsibilities as they relate to risks and threats, stakeholders need to know which tools would be most effective for performing their tasks. For example, hazardous materials teams are not the sole responders for a chemical, biological, radiological, nuclear, or high-yield explosive (CBRNE) event. They must coordinate and cooperate across disciplines to provide the most effective response and reduce the number of people exposed to toxins and other deadly agents.

In today's ever-changing threat environment, a whole community approach is the only effective approach. A rail incident is not just a rail and passenger problem, it also affects the lives, health, and productivity of all those in the local community, the surrounding communities, and the numerous communities connected physically, virtually, or emotionally with the impacted site. In a truly resilient community, stakeholders would strive to educate and equip themselves to prevent and, when needed, respond to disasters. As with links in a chain, each stakeholder must play his or her part while connecting with other agencies and organizations in order to complete the whole community resilience "chain."

Emerging Threats to Rail Infrastructure: Part II, Passenger

By Catherine L. Feinman

With millions of passengers travelling each day by rail and subway in the United States alone, the passenger rail industry and the communities they serve are faced with difficult safety and security challenges – from equipment failures to terrorist attacks. A whole community approach is needed to address these challenges, to understand the threats and consequences, and to promote a culture of resilience.

A roundtable held in New York on 9 January 2018 examined current issues and progress regarding this important topic from government and private sector experts. Key discussion points included current threats, vulnerabilities, consequences, and interdependencies that need to be addressed in order to avoid or mitigate a potentially catastrophic incident:

- Capacities in public/private sector passenger rail infrastructure preparedness;
- Local, regional, and national infrastructure resilience interdependencies involving passenger rail;
- Rail security and safety regulatory trends;
- Railroad and government partnerships; and
- Consequences of a cyberattack on Supervisory Control And Data Acquisition (SCADA) systems.

The January roundtable and its key takeaways continue the discussion that began in Washington, D.C., on 10 October 2017. At the October meeting, Joseph Trindal moderated a discussion on Emerging Threats to Rail Infrastructure: Part 1, Freight. Those subject matter experts noted the similarities and differences between threats to freight and passenger rail. The freight rail discussion raised significant concern for hazardous materials, military transport, critical infrastructure, communications, and cybersecurity. Although all of these issues are applicable to the passenger rail industry as well, there is one significant difference – people.

Passenger rail incidents increase the possibility of mass casualties, the need for public information sharing, and the importance of public situational awareness. As demonstrated in 2015 by three Americans, a French national, and a Briton travelling to Paris, situational awareness and quick action before law enforcement arrives could save lives. After the gunman opened fire in that train, these passengers subdued the suspect, provided first aid to victims, and shared valuable information about the incident to law enforcement. Unlike freight rail, the public plays a more significant role and must be included as a key partner in the planning process. Similarly, other rail passengers may find themselves someday pushed into the role of "first responder" when an incident occurs in transit. As such, incident awareness is critical even when formal training is lacking.

In addition to terrorist-related attacks, three recent Amtrak incidents – collision with a dump truck in Washington in December 2017, train derailment in Virginia in January 2018, and collision with a freight train in February 2018 – have gained national attention. Such incidents have brought public attention to the need for improvements in the rail infrastructure, protocols, and technology such as positive train control. Although public and congressional debate has been spurred by these events, the rail industry has been taking steps to address safety and security gaps for years. For example, in June 2015, Southern California's Metrolink was the first passenger rail system to implement a positive train control system across its entire network. In addition, Amtrak provides free training through its Operation RAILSAFE (Regional Alliance Including Local, State And Federal Efforts) program to local stakeholders to help build awareness among planners, responders, and the passengers who may one day be affected.

Intelligence & Security Concerns

Al-Qaida recently published the 17th volume of its *Inspire* magazine. This issue is dedicated to exploiting the U.S. rail networks for attack. Their goal is to steer potential lone actors and disconnected violent extremists to target rail systems, which includes the passenger rail network. This specific threat underscores the need for the U.S. rail transportation industry to maintain and strengthen partnerships with federal, state, and local authorities.

To begin the 9 January 2018 discussion, the moderator – James Cook, inspector in the Amtrak Police Department – put the rail security challenge into perspective with regard to financial investments. According to his former boss, he quoted, "The government spends billions of dollars to protect millions of passengers in air travel, while spending millions to protect billions of passengers in the mass transit world." Even though passenger rail threats have, to date, been more frequent outside the United States, threats of attack from terrorist groups have heightened across all developed countries. Two recent attacks did not reach their full intended potential, but still gained broad attention worldwide: (1) in August 2015, a man opened fire with an assault riffle in a train traveling to Paris, France; and (2) in December 2017, a suspect inspired by the Islamic State (IS) group detonated a pipe bomb in the New York subway.

A shift in terrorist tactics makes early detection of such threats more difficult. Large-scale coordinated attacks using chemical and biological weapons are less common than those of lone actors employing guns, knives, and improvised explosive devices against open public space targets, as demonstrated by the Islamic State of Iraq and the Levant (ISIL). However, no tactic should be overlooked. Edward Bruce, director of intelligence for the New Jersey Transit Police, shared some insight into current and emerging threats to mass transit, which can be categorized into four groups: international terrorism, homegrown violent extremists, domestic terrorism, and single-issue extremists/lone offenders.

Whether working as an organized group or as a radicalized individual without direct affiliation with a terrorist organization, the type of weapon used influences the potential scale of the event. While the use of explosives, small arms, edged weapons, and vehicles ramming pedestrians remains the prominent concern for mass transit, Bruce mentioned a potential future threat of ISIL-inspired extremists desiring to use simple improvised

chemical dispersal devices, as demonstrated in a recent plot from Australia. He explained that the plume from an improvised chemical device could be perceived as a fire-based smoke condition, which could put even more people in danger, due to a misunderstanding on how to effectively respond. Furthermore, with the rise of ISIL to prominence in 2013 and 2014, threats do not have to be transportation specific to be a concern to mass transit. Threats to any open public space venues at or near mass transit stations would raise the threats to mass transit as well – as demonstrated by the attack on the Manchester Arena, which was co-located with Victoria Rail Station. Homegrown violent extremists remain mass transit's number one threat. However, it has become increasingly difficult to collect intelligence on single-issue extremists and lone offenders who operate in an isolated manner. It is probable that intelligence on a single issue extremist or lone offender will be gathered by an employer's human resources department or by the subject's family and friends before law enforcement. People closest to that individual are likely to be the first to detect a potential threat.

Michael Gray, adjunct faculty in the Global Business and Transportation Department at the State University of New York, expressed a growing concern about ramming incidents and attacks outside hardened security areas. For example, in November 2014, a man drove a car into a crowd of people near a light rail station in Jerusalem. In May 2017, a suicide bomber attacked a crowd at an Ariana Grande concert in Manchester – British Transport Police officers and Northern Rail employees were among the first to respond. In Istanbul, where security at checkpoints has been increased, terrorists simply began moving their efforts to target crowds outside the security checkpoints.

Threat Mitigation

Information sharing and understanding cascading effects of even small incidents can help minimize security gaps. With much focus on large-scale, unconventional, less-frequent incidents, simpler tactics that are quick, easy, and productive can more easily breach security efforts such as targeted passenger screening and magnetometers. "There is currently no screening system that will screen everyone in a mass transit environment and to attempt to implement airport-style screening on mass transit would remove the 'mass' from mass transit," said Bruce. He further noted that, everyday in mass transit, the passenger levels are equivalent to or greater than a large-scale event held at a stadium or outdoor event. Any station can be a target, with times and locations of trains publicly posted. Yet, even a small incident can have a widespread devastating impact.

Thomas Lockwood, board member of the Secure Technology Alliance, highlighted that, for many people, cybersecurity is perceived as isolated and personal nuisance issues. Many do not understand potential impacts of business enterprise as well as operational products and services. For example, a brief disruption in payment systems can nearly instantly stop the flow of people and traffic; or an attack on enterprise can stop communication, information sharing, and situational awareness. For regional transportation authorities, if a system cannot be used because payments cannot be made, it would result in a significant effect on mass transport. "Big issues like terrorism are a concern, but everyday small issues like malware can have a significant impact," said Lockwood. He warned that systems today are not as isolated as they used to be, and the risks posed are critical. This is especially important for maintaining public confidence in the mass transit system.

In addition to the cascading effects of a brief cyberthreat, secondary threats can spread rapidly via mass transit. For example, biological and chemical agents pose threats to outliers, when a contaminated person travels to other locations, potentially spreading the incident to other jurisdictions. Roundtable participants agreed that boots on the ground need to know what to do in such circumstances, but building public awareness is a challenge. With regard to public awareness efforts, Bruce said, "It's not just a question of how effectively it is sent out, but how effectively it is heard." Mass transit providers focus on transporting people to their locations quickly, efficiently, and safely, while many commuters spend the time occupied with their electronic devices, wanting to just "enjoy the ride." Attitudes like this may hinder reception of public awareness efforts. The "See Something, Say Something," which began in mass transit, is effective, but only with an alert public.

Industry leaders discuss issues related to the passenger rail industry: terrorism, hazmat, critical infrastructure, communications, cybersecurity, and people.

Heightened awareness is especially important to detect precursors – or preparatory training – for a larger attack. Mass transit is inherently a complex environment with high-value targets that need to be protected. Joseph Brandine, manager of Chem, Bio,Rad Security Programs for Metro-North Railroad, stated that creating a modular "system of systems" is a good plan. However, since many detection system vendors still operate independently and proprietarily, a faster common operation software integration process is needed to address a system-wide development. Sebastian McClendon, CBRN project manager for The Port Authority of New York and New Jersey, agreed that better integration is needed to address a potential system-wide, cascading issue.

As an intelligence officer for mass transit law enforcement, Bruce has to consider both perspectives. From an intelligence standpoint, he explained that the intelligence community tends to focus on predominant (asymmetric) threats. Although adjusting focus to emerging threats can sometimes be slow, the intelligence community (both the U.S. Intelligence Community and law enforcement intelligence) is getting much better at adapting to a dynamic threat environment. From a mass transit standpoint – no matter what the incident is – terrorism becomes the initial concern and must be ruled out first, and then the focus can move down to lesser threats. It is much more difficult to shift from a smaller criminal concern to a larger terrorist concern.

CBRNE Threats & Assets

Cook raised the question about whether New York transit agencies have the resources in place to combat current threats in chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) domains. Brandine of Metro-North Railroad stated that, since 2004 when the Republican National Convention was hosted in New York City, the city has had a complex detection system in Penn Station and Grand Central Station. This system helps the metro system meet its protection goal, but funding is an ongoing challenge. On the law enforcement

side, Lt. Art Mogil of the New York Police Department, stated, "We will never have enough resources to protect *all* transit stations." He described how the city has 472 stations, each with multiple entrances, plus roughly 700 miles of track. With that in mind, he said it is necessary to conduct protective operations selectively based on intelligence, population density, etc.

Bobby Baker, captain and WMD/hazmat coordinator for Dallas Fire Rescue's Special Operations, stated that Dallas does not have a dedicated hazmat team. Although a report he cited showed that not having such a team increases risks, early identification and classification of agents can mitigate secondary threats. An integrated planning approach can bridge the "silos" (e.g., between firefighters and police officers), which make it more difficult to identify threats before or in the early stages of an incident. For example, he described a scenario where an active shooter could be used as a diversionary tactic to spread contaminants by sending contaminated victims to hospitals that are not equipped with CBRNE detection equipment. He stated that CBRNE detection should be deployed and positioned outside patient receiving facilities.

Tony Mussorfiti, lieutenant (retired) of the Fire Department of New York (FDNY), described HazMat Company 1, FDNY's dedicated hazmat team, which includes seven technician specialists and an officer, and has been in operation since 1984. The team was proficient in the handling of hazardous materials, but – after the Tokyo subway sarin attack committed on 20 March 1995 by members of the cult movement Aum Shinrikyo – the members of HazMat 1 needed to develop procedures on how to handle contaminated victims as well. To address that concern, the team used a "tiered response" (mission-specific), with specialized units to assist with rescue, recovery, and other tasks. Today, the team plays a key role in deterring terrorist incidents and lessening the consequences.

Measuring Risk & Deploying Assets

The response to low-frequency, high-consequence events needs to be more proactive than reactive, which includes rapid deployment of assets. To facilitate rapid deployment, assets need to be available and plans in place well in advance of the incident. "We don't watch a bunch of houses burn down before we install smoke detectors," said Baker to emphasize the point that an incident that could be mitigated with the proper resources can turn catastrophic without them.

The question is how to measure risk and determine where to deploy assets. Just a few of the numerous risk factors include the quantity of people affected, impact on the economy, and criticality within the overall system. With regard to counterterrorism and risk management, Bruce stated, "Threat is a frequency issue, but risk is a larger cost and response issue. Threat is one factor of risk." He explained that a threat may be something that is likely to occur, but when considered alone, it might not tie into the vulnerabilities or address the consequences (e.g., cost to mitigate). When addressing a high-consequence concern, it is critical for intelligence-led agencies to balance resource allocations by considering the use of risk-based planning.

Planning gaps related to risk (e.g., updating protocols, coordinating with neighboring jurisdictions) must be addressed. Ken Metz, inspector for Amtrak Police New York Penn

Station, described how his agency performs risk management for certain buildings, listens to intelligence reporting, considers baselines and best practices, learns about emerging threats, and then re-evaluates these facilities. Even when the railways themselves are not affected, an incident can affect the finances of the company, people entering the buildings, and how people travel. When a new threat is introduced, he said it is time to re-evaluate the trains, stations, or yards to ensure the threat is mitigated.

Stakeholder Roles, Partnerships & Information Sharing

The next topic of discussion turned to the roles that stakeholders play, their partnerships, and the way they share information. "The relationship factor is where things go forward," said Baker.

According to Metz, Amtrak works with a lot of state and local partners through Operation RAILSAFE. The concept of this alliance is to increase the number of law enforcement officers at stations, which provides an opportunity for the officers to exercise their counterterrorism and incident response capabilities. Such networking efforts also promote higher involvement as needed when an incident occurs. Being able to see each other and work together on a regular basis improves stakeholder involvement.

Fusion centers and the Federal Bureau of Investigation's (FBI) Joint Terrorism Task Force (JTTF) help to build relationships within the intelligence community. The FBI also has a rail security coordinators program, where each FBI office has a rail security coordinator within the JTTF. This coordinator ensures that connections and intelligence are shared with the right people. In New York, integrating the fire services into the JTTF has also improved coordination for responses.

Constant communication and networking are critical at the tactical level as well. Spearheaded by the NYPD, Mogil described how the Securing the Cities Program helped identify a gap in capabilities. As a result, the program implemented common equipment, settings, training, and terminology, which facilitate the intelligence-sharing process. By communicating frequently, gaps in resources can be identified early, and mutual aid can be implemented efficiently.

With much of the discussion focused on New York City, Rick Mathews, Public Service Professor at the University of Albany, pointed out that mass transit discussions often focus on big city assets. However, much of the rail transit system goes through small and rural areas, where jurisdictions may not train as well together at the group level. Interoperability needs to be encouraged across both large and small jurisdictions. He noted that plans for an attack on mass transit within a big city like New York would encounter barriers already in place. However, lack of such barriers in less populated areas would have greater vulnerabilities (e.g., a terrorist boarding a train in a small unguarded station and traveling into a large, heavily populated station).

Even with Amtrak's outreach efforts across the jurisdictions that rail lines cross, repetition is critical. Metz said that, "Doing it once does not mean success. It needs to be done repeatedly." Chuck Frank, director of emergency management and business continuity

at Metropolitan College of New York, said that his university uses a "constructive action" process to help create and implement emergency plans. However, he also noted that stakeholders may reprioritize changes based on what is *perceived* as the greatest threats and risks, rather than what the greatest threats actually are. For example, the *Inspire* magazine article on rail threats captures the public's imagination, but actions to mitigate them without using a holistic approach may be misguided.

In addition to different perceived risks and threats, each state and jurisdiction has a different way of conducting operations. Although these differences need to be recognized – especially considering that rails and buses transverse jurisdictions – agencies cannot wait for training before they become well acquainted with other key stakeholders.

After 9/11, fusion centers helped stakeholders understand roles and request information and protocols, but key interdependencies are sometimes underestimated. Withholding information or releasing it at the wrong time can have significant impacts. Similarly, releasing different organizational perspectives can cause further disruption. It is important to think about how people understand basic incident management coordination and information sharing because, as Lockwood witnessed in several incidents, the private sector has yet to embrace or be fully integrated into the process.

Strategic alliances and partnerships are one way to address the issue that every agency lacks some resources. Robert Black, senior associate of operations at Applied Integrated Security, shared the example of the U.S. Coast Guard (USCG) having operational and strategic memoranda of agreement (MOAs) with many local communities to fill capability gaps and to build force multipliers (e.g., law enforcement functions, environmental protection and enforcement, critical infrastructure security).

Similarly, Amtrak's Operation RAILSAFE addresses security over the ground, air, and water through alliances with state and county aviation units. Through these partnerships, law enforcement officers gain coverage from an aerial perspective while using the opportunity to

educate the pilot and copilot on law enforcement aspects of the rail system. Amtrak also has maritime alliances with the USCG and other law enforcement agencies.

Bruce stated that it would be difficult to respond to a law enforcement incident in New Jersey without having to work well with other agencies. Cooperation and joint operations are critical. As such, coordination is imperative. The NJ Transit Police Department regularly coordinates with Amtrak PD, MTA PD, PAPD, NJ State Police, NJ OHSP, FBI, TSA, DHS, and many other key stakeholders. From the law enforcement and emergency response perspectives, the jurisdictional conflicts seen in past decades are in the past, and the concepts of joint operations and unified command are integrated into daily operations.

Resilience Drivers

Roundtable participants then discussed how agencies should consider how they would continue functioning when one rail line or one operational component is removed. For example, one previous Amtrak incident had an ultimate $45-million impact on the U.S. economy. For a systems architecture, the process needs to build in both security and resilience to avoid having a single point of failure.

It is difficult to retrofit resilience. For example, although some train tunnels need repair, there would be significant economic impacts if one were to be shut down temporarily (which could be for years) for repair. Law enforcement officers, for example, do not build the tracks, but they are tasked with ensuring that the security process is streamlined across various jurisdictions. Getting critical assets to the scene when there is resistance to move those assets can be facilitated with the right planning and networking (e.g., police escorts for concrete trucks to lessen red tape delays).

Many decision makers do not participate in high-level exercises, even though they are involved in strategic decision-making during an incident. The problem is determining how to create a good mechanism to make these decisions, and exercise and train the decision makers. This includes having a government structure that embraces volunteers to overcome funding gaps and overwhelmed agencies. This was seen during Hurricane Harvey in 2017, when the Cajun Navy filled the response gaps despite not being included in the disaster planning process.

The NYC Emergency Management Department streamlines its decision-making process by working closely with all city agencies, nonprofit and nongovernmental organizations, and state and federal agencies. In addition to traditional stakeholders, NYC Emergency Management also works with Community Emergency Response Teams (CERT), Voluntary Organizations Active in Disaster (VOAD), and its Ready New York program to promote volunteerism within the city. “Volunteers are the richest resource,” said Anita Sher, assistant commissioner for the Training & Exercise Division at NYC Emergency Management. To address gaps in training the decision makers, NYC Emergency Management has moved away from large-scale exercises to smaller more-frequent training and tabletop exercises. This approach brings in senior-level people to help them better understand their obligations and roles during critical incidents.

Black mentioned a high-level tabletop exercise (TTX) that was held by USCG Sector NY, notably involving the Mayor's Office, NYC OEM, the Captain of the Port, the Port Authority heads, top level law enforcement, and senior emergency responders, among others. In the TTX scenario, hijackers had seized a chemicals tanker just above the Verrazano-Narrows and were holding the region hostage. The tanker had two separate but stable chemical cargoes which, when mixed, would become a city-leveling mass destruction explosive. The scenario fully engaged in play the metropolitan area's highest-level federal, state, and local decision-makers. The TTX outcome was considered a success but remains one of only a few that have been run.

Funding challenges are compounded when there are misunderstandings about natural disasters versus terrorist-related disasters. Baker pointed out that terrorism, which requires a presidential declaration for appropriation of funds, does not qualify for the Stafford Act, which typically falls under natural disasters. As such, expected funding may not be available. In such cases, the economic impact becomes exponential, so volunteers become even more critical.

Another way to bridge the gap between agencies and organizations is to use standards and procedures such as the Incident Command System (ICS) and the National Incident Management System (NIMS), which offer free online training to build continuity between agencies and organizations. As such, many incidents have become ICS driven. Baker noted that, in one Texas team leader course for preventing radiological and nuclear disasters, part of the training involved building an incident action plan and ensure the ICS/NIMS forms are filled out correctly. Mussorfiti added that, although NIMS compliance is needed for some funding, OSHA, NFPA-475, and other documents could provide critical backing for resource and equipment needs that could help build resilience.

Resilience and incident response, of course, are not the same. Bruce stated that he believes major incident responses are done well, but resilience involves putting systems in place to prevent incidents from having such a large impact. When considering resilience and interdependencies, Bruce said, "We still have large gaps to overcome…. We need to build robust systems that can flex around an incident." As an example of misunderstanding resiliency, he described an incident in the Port Authority Bus Terminal that prevented buses from entering. This is an example of a short-term response effort by redirecting the buses, but he would not consider that a resiliency program.

Resilience looks at how robust the system is and how much an incident will affect the system. Robert Bradley, battalion chief (retired) at Middletown CT Fire Department and a senior instructor at Louisiana State University and National Center for Biomedical Research and Training, described one challenge with meetings and training: emergency managers and emergency responders go to critical incidents in the initial phase, and then go home, while others are tasked with rebuilding and recovering. The missing steps are identifying, connecting (and staying connected) with, and getting the infrastructure and other private sector people involved. Building these relationships can be difficult because their time and systems cost money, but long-term resilience and long-term cost savings are difficult without it.

"The bulk of risk agencies carry often comes from a lack of resilience, making unique assets more critical to their operations," said Bruce. Though entities charged with developing infrastructure do consider resilience, they may benefit from further coordination on resiliency with emergency preparedness and response communities. Bradley agreed that gap analyses can help identify training components, but they too need to be expanded and built upon.

A lot of mass transit infrastructure is aging or old and, regardless of the type of incident, outdated infrastructure has an impact. Without fixing and updating these structures and standards, some response efforts cannot be as effective.

Information Sharing

"Effective resiliency requires effective redundancy," said Tim Stickler, director of CBRNE protection technology at Federal Resources. This statement could be applied to equipment and other resources, funding streams, and information sharing. Interdependencies and resilience efforts have ripple effects across the country, even when incidents are local. The intelligence community is moving rapidly to address these concerns.

After an incident, restoring operations begins immediately. However, when a major event occurs, each agency puts out perspectives from its agency. As a result, too much information can become "white noise," said Cook. There needs to be a determination of what is considered "good intelligence."

There has been a maturing of the intelligence sector, which now realizes that capabilities exist within many different sources. Bruce has noticed that the "walls" between intelligence and law enforcement have been coming down. However, distributing information to the lowest level can still be challenging. The goal is to get as much information to the boots on the ground. To do so, commanders need to be able to share information whenever needed. Therefore, ensuring that operations and intelligence work closely is critical, so that information is unified and sent with a common purpose.

There is enough information at the unclassified level that can be shared to successfully steer operations and inform situational awareness. There has been growth on the operations side as well. Commanders and officers now understand that intelligence is a two-way flow of information, which is critical to improving both intelligence collection and dissemination.

Technological & Regulatory Influences

The roundtable discussion then turned to the feasibility of a cyberattack on mass transit and the steps that have been taken to prevent an attack. In the rail industry, cyber influences can often be overlooked. It is easy to remember bombs and other physical threats, but cyberthreats are not always at the forefront of planning efforts. How people prepare for cyberthreats can vary significantly as well. Black, who is also a member of the InfraGard's EMP Special Interest Group, stated that cyberattacks certainly are feasible because of the integrated systems of computers, communications, and the national electricity grid.

Although the threat is real, there are actions that individuals can take to mitigate the threat. On the ground level, for example, each person has a responsibility to not expose passwords, which can invite threats. Password protection and two-factor authentication on

computers and keypads guard critical information. Protecting credit cards and other financial information is also a significant concern.

Years ago, operational and business systems were isolated and separate systems. However, since the 1980s and increasingly over time, these systems became interdependent and interoperable. This integration provides multiple areas of risk and potential attack. The increasing use and integration of third-party providers and unauthenticated systems create vulnerability because access to one system may provide access to another. With the "internet of things," an accounting of transactions is required, but security elements have not been stressed. More security requirements – including multi-factor authentication, mandating third-party access requirements, and other protections to reduce cyberrisks – are needed. The points of entry for cyberthreats are numerous, so security gaps need to be addressed. A May 2016 report conducted by the Preparedness Leadership Council International provides some recommendations.

Resilience can be expensive when done in retrospect, but it can be relatively inexpensive if built into the structure and process upfront. Fixing the problem is a challenge because, "When it's everybody's problem, it's nobody's problem," said Lockwood. However, Lockwood did provide the following suggestions:

- Determine how the public and private sectors are structured to share information
- Create opportunities to get cyber leaders together to talk in trusted environments
- Include cyber-related issues and private sector within exercises
- Identify gaps in information sharing, common understanding of risk, prevention, resiliency, and recovery strategies
- As cyberthreats change, change cyberprotection as well
- Promote minimum requirements and understanding of contractual requirements for third-party organizations
- Encourage adoption of security guidelines and standard requirements
- Offer internships as cyber analysts in fusion centers
- Understand that each person must take some responsibility

Key Takeaways

Passenger rail security has to adapt as threats against railroads and the surrounding areas evolve. The roundtable participants discussed various threats that could affect the rail system and possible solutions for closing security and resilience gaps. Some of the key takeaways from the Emerging Threats to Passenger Rail Infrastructure roundtable discussion include:

- **Terrorist tactics are shifting** – Through outlets like Inspire magazine, terrorists have overtly expressed an interest in targeting and disrupting rail travel, and have provided instructions on how to do so. Lone actors with conventional weapons are more likely than large-scale chemical and biological attacks.

- **Threat perceptions can influence incident scale** – When people do not recognize a threat (e.g., a toxic plume), they may not take measures to avoid it or may even approach it. Similarly, better education, warning systems, and information sharing could lessen any threat's impact.
- **Non-rail threats can become rail threats** – When areas surrounding rail infrastructure are compromised, it can have cascading effects on the rail system. Similarly, secondary threats like contaminants can be transported quickly via rail, thus expanding the incident.
- **Small threats can become big threats** – A threat to a small rural station can lead to consequences throughout the rail network. In addition, a cyberattack within the rail system can affect traffic patterns and payment systems, cause significant delays and closures, and influence operations of other agencies and organizations in the surrounding area.
- **CBRNE detection needs more integration** – CBRNE detection measures have been implemented in some high-risk areas, but it is not possible to have specialized teams and equipment in all areas of mass transit. Better integration between hazmat teams and other responders would serve as a force multiplier in early identification of potential threats.
- **Planning gaps increase risk** – Planning involves a never-ending cycle of assessing, learning, implementing, sharing, and re-assessing. Risk assessments, best practices, MOAs, and two-way communication are just a few ways to help close planning gaps.
- **Public awareness continues to be a challenge** – With the broad use of technology such as cellphones and tablets, situational awareness may not be practiced and potential threats may go unnoticed. Pushing information to the public does not guarantee that the public will hear it. Repetition is key and messaging from multiple agencies must be coordinated.
- **It is better to build in resilience than to retrofit it** – The rail infrastructure is aging and sections will soon need to be replaced. Decision makers should be proactive and consider long-term resilience versus short-term cost savings. Lack of resilience creates risk.
- **Decision makers need to be involved in training** – Senior-level stakeholders understand their roles and responsibilities during daily operations, but they also must be aware of how these can change during critical incidents. Smaller, more frequent training may engage them more easily than large-scale exercises.

Conclusion

Passenger railroads could be a desirable target for terrorists because of the high-volume of passengers and interconnected rail lines that span the nation. The ripple effect of a cyberattack on the ticketing system, a conventional attack in a busy train station, or a biothreat in a train car could have devastating consequences. The intelligence, law enforcement, and transit

communities are adapting to address these and emerging threats, but terrorists continue to evolve their tactics with each new security effort. Risk assessments, interagency and public-private partnerships, cybersecurity measures, CBRNE detection technology, training at all levels, information sharing, and long-term planning are ways to build resilience and security into the rail infrastructure.

DomPrep would like to thank Federal Resources, who sponsored the 9 January 2018 roundtable discussion in New York. Also a special thanks to all those who participated in that discussion, upon which this white paper is based. The participants who contributed to this important discussion include but are not limited to the following:

Bobby Baker, *Captain, WMD/HAZMAT Coordinator, Dallas Fire Rescue, Special Operations*

Robert Black*, Senior Associate/Operations, Applied Integrated Security*

Robert Bradley, *Battalion Chief (Retired), Middletown CT Fire Department, and Senior Instructor, Louisiana State University, National Center for Biomedical Research and Training*

Joseph Brandine, *Manager, Chem, Bio, Rad Security Programs, , Metro-North Railroad*

Edward Bruce, *Director of Intelligence, New Jersey Transit Police Department*

James Cook, *Inspector, Amtrak Police Department*

Patrick Dempsey, *Senior Sales, Federal Resources*

Chuck Frank, *Director, AA/BA Undergraduate Program, Emergency Management & Business Continuity, Metropolitan College of New York*

Michael Gray, *Adjunct Faculty, Global Business and Transportation Department, Maritime College, State University of NY*

Thomas Lockwood, *Board Member, Secure Technology Alliance*

Rick Mathews, *Public Service Professor, Department of Public Administration & Policy, University of Albany, and Principal of The Mathews Group LLC*

Sebastian McClendon, *CBRN Project Manager, The Port Authority of New York & New Jersey*

Ken Metz, *Inspector, Amtrak Police New York Penn Station*

Art Mogil, *Lieutenant, New York Police Department*

Tony Mussorfiti, *Lieutenant (Ret.), Fire Department of New York, and current member of Advisory Council for Commissioner Nigro of the FDNY*

Aaron Poynton, *Executive, Federal Resources*

Anita Sher, *Assistant Commissioner, Training & Exercise Division, New York City Emergency Management Department*

Tim Stickler, *Director of CBRNE Protection Technology, Federal Resources*

Erica Wolfkill, *Manager: Federal Government and Critical Infrastructure, Federal Resources*

Catherine L. Feinman, M.A., joined Team DomPrep in January 2010. She has 30 years of publishing experience and currently serves as editor-in-chief of the DomPrep Journal, www.DomesticPreparedness.com, and the DPJ Weekly Brief, and works with writers and other contributors to build and create new content that is relevant to the emergency preparedness, response, and resilience communities. She also volunteers as an emergency medical technician, firefighter, and member of the Media Advisory Panel of EMP SIG (InfraGard National Members Alliance's Electro-Magnetic Pulse Special Interest Group). She received a bachelor's degree in international business from University of Maryland, College Park, and a master's degree in emergency and disaster management from American Military University.

Protecting Food, Air, and Water: Environmental Health

On 22 March 2018, DomPrep Advisor Andrew Roszak spoke with Dr. David Dyjack, director of the National Environmental Health Association (NEHA), about the field of environmental health as it relates to disaster response and mitigation as well as overall community resilience. Unlike public health, which specializes in the social and policy realms, the field of environmental health is scientific and technically oriented to ensure that communities are safe from various environmental contaminants and allergens.

Incorporated in 1937, NEHA currently serves 5,000 "boots-on-the-ground" environmental health professionals located across the United States. At the intersection of environmental health and disaster response, these "second responders" minimize risks as people return to their homes and offices following disasters. For example, when flooded superfund sites contaminate drinking wells or hurricanes and floodwaters cause mold contamination, these professionals ensure safe practices for refuse disposal, temporary food kitchens, clean water, emergency shelters, and mass casualty management.

Perhaps the greatest challenge for the environmental health field going forward is the issue of clean water, which can be overlooked until it is not available. Too much or too little water pose problems too. Managing the water supply with an aging water infrastructure requires careful planning to ensure that water is being used effectively, conserved, and protected to combat risks associated with the extremes of flooding and drought. With these and other environmental challenges, a degree in environmental health provides innumerable opportunities in today's society. "Environmental health is profoundly local," said Dyjack, and their technical expertise is important at all phases of a disaster.

Learn more about NEHA at http://www.neha.org or connect directly with Dr. Dyjack on Twitter @dtdyjack.

Click to listen.

Andrew Roszak, Moderator,
Senior Director for Emergency Preparedness, Child Care Aware® of America

David Dyjack
Executive Director and CEO, National Environmental Health Association (NEHA)

User Guide for Responder-Driven Technology Development

By Ann Lesperance & Richard Ozanich

With new technology coming to market at a record pace, it can be difficult to know whether products are reliable, durable, and secure enough to make the nation's emergency management professionals safer, better connected, and fully aware. The market is flooded with tools and capabilities that may be of benefit to first responders, but these tools need to be vetted for the rigorous technical, operational, and safety needs in the field.

To ease the vetting process for new technology, Pacific Northwest National Laboratory (PNNL), on behalf of the U.S. Department of Homeland Security (DHS) Science & Technology Directorate (S&T) First Responders Group (FRG), created a user-friendly, streamlined approach to partner with technology developers. This partnership lets users test technology products and then actively use their feedback to drive future development. It is called the First Responder Technology Operational Field Assessment (OFA) and comes with a guide to assist users through the process.

First Responder Technology Operational Field Assessment

The OFA enables diverse organizations to assess technology products in a credible, consistent, and verifiable way. The *First Responder Technology OFA User Guide*, available on the DHS S&T website, guides a "technical facilitator" in how to partner with technology developers, first responders, and subject matter experts (SMEs) to evaluate a product's applicability and usability in the intended environment and with a designated organization. Accompanying the guide are user forms and templates that can be modified to fit different technology products, scenarios, and use cases.

The OFA process is designed to gather user feedback to better understand the constraints and technology needs of first responders (the intended end users), and then use that input to drive technology development. PNNL designed the OFA process and user guide in partnership with DHS S&T FRG, first responders, and SMEs from across public and private industry and academia, and then vetted the approach via a working group of leaders in the field.

Three-Phases Drive User-Centric Approach

The resulting OFA process comprises three key phases:

- *Phase 1 – Technology Profile.* A technical facilitator (a designated organization overseeing the OFA) partners with a technology developer to complete a technology profile that captures a technology product's technical and operational specifications. The profile is then translated into user-friendly information products that are validated with first responders and SMEs. This creates a baseline of information to be used throughout the OFA.
- *Phase 2 – Technology Introduction & Feedback.* The technical facilitator validates the technology profile with first responders and SMEs and incorporates their

feedback. This prepares the team to conduct the OFA and pilot the technology product in the field.

- *Phase 3 – Technology Field Demonstration.* The technical facilitator and technology developer conduct the OFA and assess the technology product, ideally in multiple progressive, real-world operational settings with the intended end users.

Field-Tested With Realistic Scenarios

In February 2017, PNNL partnered with staff at the Xfinity Arena in Everett, Washington, to pilot the approach and demonstrate a communications and enhanced situational awareness technology that was part of the DHS S&T EMERGE accelerator program. Event staff used the technology (app, smartwatch, cellphone, tablet) during a hockey game at the Xfinity Arena, a 10,000-seat venue. The selected users included a command center lead, four security team leads, a law enforcement representative, and an Emergency Medical Services (EMS) technician.

During and after the event, interviews were conducted with the users on the technology product, asking how the product met their expectations, how it operated and met their needs in the live work environment, and what could be improved. Overall, the participants responded positively to the process and the technology, indicating they would be interested in the product with modifications, many of which the developer intends to incorporate into its software and product capabilities.

Feedback Drives Responder-Driven Technology Development

Overall, what differentiates OFAs from previous efforts is that it builds on a proven iterative – or "spiral" – approach that ensures mutual benefits. For example, technology developers gain early feedback to optimize their products for better market positioning and usability, whereas first responders provide feedback that drives product features to better align with their needs and requirements in the field.

This work was funded as part of the DHS S&T Responder Technology Alliance in which PNNL is partnered with DHS S&T FRG to envision first responder needs for the next 10-15 years and to accelerate the development of, and bring to market, integrated technology solutions that will significantly improve the safety and capability of first responders. In 2018, PNNL will be conducting OFAs to evaluate technology components that emerge from the project, including a patient monitoring sticker and EMS cuff currently in development to assist with continuous vital sign monitoring of patients.

Questions about this process or interest in conducting an OFA should be directed to the OFA team leads, Ann Lesperance at ann.lesperance@pnnl.gov and Richard Ozanich at richard.ozanich@pnnl.gov

Ann M. Lesperance (pictured above) has been with the PNNL since 1990. She is currently the director of the Northwest Regional Technology Center for Homeland Security in Seattle, Washington. She develops regional programs to accelerate the demonstration and deployment of new homeland security technologies. She works with state and local emergency responders and public safety officials to understand and prioritize their operational needs and requirements. She also builds regional coalitions of emergency management professionals to partner with Department of Homeland Security Science and Technology Directorate, the Department of Defense, and other federal agencies.

Richard M. Ozanich, Ph.D., has worked in the chemical and biodetection fields for over 25 years. He is a subject matter expert in biodetection and optical spectroscopy with a broad base of knowledge in chemistry, biology, and measurement instrumentation. He is active in the area of bioresponse and development of standards and best practices and is a member of American Society for Testing and Materials Committee E54 on Homeland Security Applications. His research includes development of automated fluidics instrumentation and microparticle-based methods for sample preparation and rapid detection of biothreats.

The Key to Saving Lives in CBRNE Events

By Bobby Baker

In January 2018, in New York City, a group of professionals – representing entities including the Department of Homeland Security, private contractors, hazardous materials/weapons of mass destruction (hazmat/WMD), law enforcement officers, and intelligence experts – gathered to discuss the emerging threats to U.S. passenger rail service. Not only are these threats pertinent to passenger rail service, but they also may potentially affect all mass gatherings and large venues across the country on any given day. Emergency planners and responders must determine the best way to mitigate such threats.

Although any attack on a mass gathering would be catastrophic, passenger rail service presents a far more complex challenge. With widespread and frequent use by millions of passengers each day – coupled with distinct access to other forms of the critical infrastructure matrix – a chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) event affecting mass transit would immediately affect passengers and require significant recovery investment, further influencing the financial impact of such a catastrophe.

The Department of Homeland Security lists 16 major categories of critical infrastructure in its matrix – of which, mass transit is just one. Despite all its benefits, the fact that passenger rail service has contiguous access and/or direct access to other critical infrastructure in U.S. communities further complicates and increases the importance of prevention. This persistent, challenging dynamic makes the prevention and response to incidents involving passenger rail service a major hurdle for most departments' daily operations.

Protection Measures & Deployment Models

In addition to prevention and protection of the actual access venues themselves (such as Penn Station in New York and or Union Station in Washington, D.C.), communities must also protect the other critical infrastructure that these passenger rail lines connect. Protection measures must extend to passenger trains and rail lines serving local and national rail services that run above and below ground in major cities' urban central business districts. Protecting these venues and surrounding entities with physical security measures remains a priority to be considered not only in the context of traditional security and law enforcement routines, but also active shooter and other unconventional threats to U.S. cities.

Today's special event security planners employ a concept called Joint Hazard Intervention Teams (JHIT) for deployment in protecting major special events across the United States. This popular deployment model brings multiple emergency services' metrics together to form an all hazards detection and mitigation team. Although this model is not a new concept to

special events and events rated with the Special Event Assessment Rating (SEAR) around the country, this deployment model is not commonly utilized on a daily basis for the protection of critical infrastructure. Implementing this concept with specially trained cross-metric first responders in a unified command concept is the missing link in the early detection and classification of a CBRNE attack.

Whether the threat emanates from homegrown violent extremists or foreign terrorist groups, the deployment model would be comprised of multiple, specially trained individuals. These individuals would be trained and sorted across categories including:

- Counterterrorism;
- Hazmat/WMD technicians for early CBRNE detection, classification, and early mitigation tactics;
- Law enforcement officers for interdiction, arrest, and force protection.
- Intelligence analysts in the command post.
- Tactical paramedics who are specialized toxicological medics with countermeasures to combat CBRNE attacks and early trauma intervention.
- Explosive ordinance disposal experts with ordinance detection canines.

These small teams allow for assessment of an incident at the lowest possible level without interruption of the event itself. This approach allows venues, such as large daily gatherings, to be more resilient in a proactive response model rather than the usual mundane and antiquated response model commonly seen in the United States.

Early detection and classification is key to saving lives in chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) events.

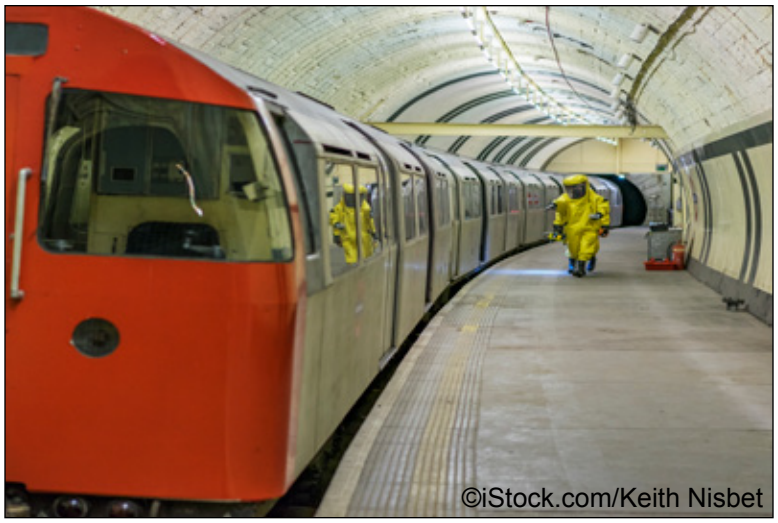
In this deployment model, if the team makes the determination after a quick screen and assessment process that a full-scale response and/or evacuation is necessary, the team leader would notify the incident command post with the level of assets needed to mitigate the situation as safely as possible to prevent further escalation and harm to the people and the venue. Overall, these assets allow daily response forces to continue service as usual without putting excess stress on resources in other parts of the city. This deployment model would ultimately save lives and resources, promoting a common balance that most incident commanders and emergency managers seek.

A Real-World Solution for Asset Protection

As more data become available about emerging threats to critical infrastructure, the need for quick and decisive preventive countermeasures will increase to meet the growing

demand for such countermeasures in public venues. Protecting the public from population and critical infrastructure perspectives are vital components to incident stabilization.

The Joint Hazard Assessment Team (JHAT)/JHIT models should be deployed into critical infrastructure locations such as passenger rail terminals, federal buildings, airports, and shopping malls to provide local jurisdictional authority the ability to detect and classify the actual threat, whether it be chemical, biological, radiological, nuclear, or explosive. The faster the local assessment team can deploy detection and classification monitors and provide feedback to the local emergency operations center and fusion centers; the more lives would be saved, and the faster critical infrastructure could bounce back and remain vibrant from an economic standpoint.



This JHAT/JHIT model should be deployed in a daily, unified command under the National Incident Management System (NIMS) nomenclature and each team should deploy encrypted communications with predetermined channels under the daily incident action plan. Before each operational period, the unified command would present any credible and general threats to the venue and/or subjects present in the venue and would conduct a site safety plan and review the event action plan. This model brings a real-world solution utilizing highly trained assets from the local jurisdiction to form a preventive all hazards team that can immediately transition to a response and mitigation team. This concept would offer every major Urban Areas Security Initiative (UASI) city the ability to protect both physical assets and human assets at a high level.

Scientific Technology & Resilience

This deployment model would bring much-needed resilience to passenger rail terminals and airports such as Grand Central Station, Penn Station, Union Station, and all major aviation hubs around the United States. These teams would detect radiation and provide early warning and prevention using radiological exposure devices or radiological dispersal devices – in a prevent passive detection mode with the ability to transfer into a response and survey mode in the event of an IED or other dissemination tool that could be used to target a venue. The ability to rapidly distinguish between naturally occurring radioactive materials and medical radiological isotopes by constantly conducting area inspections of these critical venues only adds to the overall security measures in place.

Such teams can also carry chemical warfare agent detection equipment and basic sampling equipment to sample solids, liquids, and gasses. This allows them to give a quick classification of the incident and report efficiently. Adding a biological detection capability within field polymerase chain reaction (PCR) could help classify and prevent the presence of biological incidents such as Ebola and anthrax. However, these threats could cause a widespread economical shutdown of a public transportation system and/or office buildings while waiting for the screening process and assets to be delivered to the scene. These teams would have the ability to give incident commanders a quick and scientific process to determine whether or not to protect in place, evacuate, and/or transport to local hospitals. This delivery model offers a proactive and scientific approach to consequence management utilizing the best-trained personnel and detection equipment available. Public safety sampling and the ability to rapidly deploy accepted scientific technology to give the incident commander a public safety decision matrix is quickly becoming an accepted and best practice among first responders and hazmat teams nationwide. Having law enforcement capabilities allows the team to interdict and detain individuals or coordinated terrorist groups that pose possible threats.

Combining the capabilities and technological assets of major cities should be at the top of the next resilience list. Focus on passenger rail service is an important part of critical infrastructure planning to ensure an enjoyable and safe environment that many people expect. Community stakeholders should collaborate with local emergency management teams and emergency response entities to discuss the prevention deployment model and utilize it on a daily basis to protect high-traffic areas and critical infrastructure, where incidents may become mass casualty events. Utilizing these highly trained assets in a proactive manner, rather than waiting for an incident, could be the key element to saving countless lives due to the constant synergy created by deploying and training together on a daily basis. Emergency planners should examine the critical infrastructure within their jurisdictions and determine whether deploying this model could break down the emergency response organizations' silos.

Captain Bobby Baker is a 20-year veteran of Dallas Fire Rescue and currently serves as the WMD/HAZMAT coordinator for the Dallas Fire Rescue Department Special Operations Division. He also is the founder and president of Emerging Threat Solutions LLC in Dallas, Texas. He currently serves on: the NCRP 179 Dosimetry for First Responders commentary committee; the FEMA-CBRNE Chemical Operations Support Specialist advisory panel; and the Texas State PRND advisory committee with the Texas State Homeland Security division. He is very active with the Department of Homeland Security SAVER program, in conjunction with the National Urban Security Laboratory in New York City. He holds numerous critical infrastructure protection certifications and incident management of WMD events from the Department of Homeland Security. He is a graduate of the FEMA Radiological Operations Support Specialist program and serves as an instructor for the Counter Terrorism Operations Support at the Nevada National Security Site. He holds a Master Fire Fighter certification and certified Hazardous Materials Technician through the Texas Commission on Fire Protection and is a certified Incident Safety Officer through the National Fire Academy and the Texas Commission on Fire Protection. He is a Pro-Board certified NFPA 472 Incident Commander of Hazardous Materials Incidents.

Rail Threats & Interdependencies – Thoughts for Discussion

By Rick Mathews

In the United States, there are ongoing efforts to protect the nation's critical infrastructure. Presidential directives, coupled with national security strategies and several iterations of the National Infrastructure Protection Plan (NIPP), have spanned the terms of at least four presidents and included the rail system. The volume of activity on or near rail lines, potential threats, and interdependencies all raise concern for the protection of this critical infrastructure asset.

The NIPP has been organized along general and sector provisions – with the former pertaining to aspects of the plan that should be applicable across all sectors and the latter focusing on individual factors of each specific sector. The number of separate sectors has varied, with the 2006 NIPP delineating 16 sectors, which was increased to 18 in the 2007-2008 update. In 2013, the number of sectors was realigned with the result being 16 sectors, which was continued in 2017. Although the number of sectors varied, all have identified transportation systems as being one of them. Within the Transportation Systems Sector there are currently seven key subsectors. Rail transportation is addressed in two of the subsectors: (1) mass transit and passenger rail; and (2) freight rail. According to the U.S. Department of Homeland Security (DHS) through the NIPP, there are over 138,000 miles of active railways, 1.33 million freight cars, and approximately 20,000 locomotives. The railways handle more than 12,000 trains daily.

With respect to passenger rail operations, DHS has indicated that the nation's mass transit systems provide over 10 billion passenger trips annually. Within that statistic, Amtrak accommodates approximately 31.3 million passengers annually, which is an average of about 85,700 passengers riding more than 300 Amtrak trains each day. This does not include the passenger transportation being provided by local and regional rail carriers or light rail systems.

Current & Emerging Threats

One of the differences between the two subsectors is "what" is being transported. In one subsector, the primary cargo being transported is freight and related non-human products. In the second subsector, the primary "cargo" is humans. Although freight trains also transport crews and passenger trains transport some packages, major differences remain. Considering the entirety of the two sectors – mass transit/passenger rail and freight rail – the number of potential threats can be significant. The many threats can be categorized as follows:

- Those that are caused by or are acts of nature,
- Those caused by mechanical failures,
- Those directly related to human acts – either by accident or on purpose, and
- Those caused by system failures due to interdependencies

It can also be useful to group threats according to the threat's specific target, for example:

- Threats to the railway itself, or to bridges being crossed;
- Threats to the terminals where passenger board and disembark;
- Threats to the human operation of a train or perhaps to the supervisory control and data acquisition (SCADA) systems that comprise its operational controls; or
- Threats due to lack of fuel to energize the locomotive, with the deficiency being a consequence of supply chain interruptions caused by storms or other threats to the fuel system.

In other words, to do a comprehensive analysis of the threats to the railway subsectors, one needs to think in a broader scope than one might otherwise undertake.

Interdependencies (With Passenger Railways & Systems as the Base)

Many published papers and articles have addressed the concept of interdependencies and how they relate to critical infrastructure systems. A paper published in 2006 by the Idaho National Laboratory (INL) spoke directly to this point. The purpose of the underlying research was to survey literature related to U.S. and international research in interdependencies. The paper cited a quote from the 2002 Congressional Research Service Report for Congress, "The Nation's health, wealth, and security rely on the production and distribution of certain goods and services," which is the basis for the term "critical infrastructure" (CI). The relationships among different sectors of critical infrastructure were not significantly studied until the mid- to late 1990s. One of the consequences of this has been an "incomplete understanding of the interdependencies between infrastructures," as quoted from a 2002 RAND report cited in the INL 2006 paper.

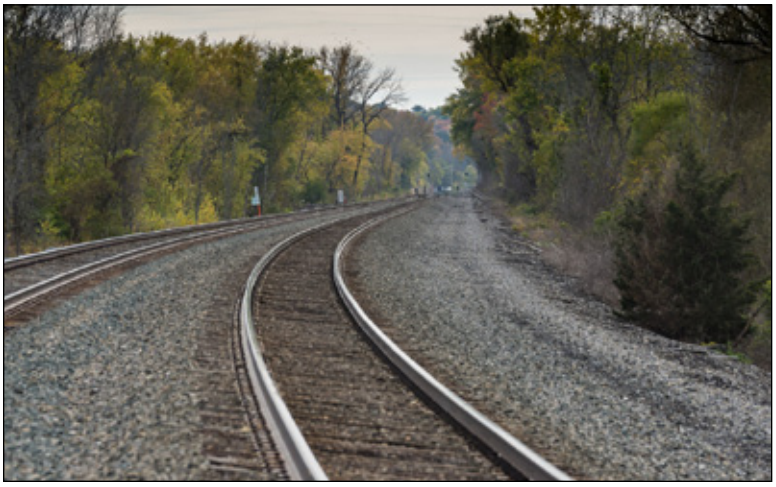
How should emergency preparedness and response professionals think about critical infrastructure protection?

Since the late 1990s, research and papers have been published defining and discussing the concept of interdependence and how this relates to critical infrastructure. Some characterize dependencies by category such as physical, cyber/informational, geographic/geospatial, policy/procedural, and societal. The takeaway is that once a classification system has been adopted, the relationships among CI sectors and subsectors can be examined.

One Hypothetical Scenario

Assume one autumn day, a passenger train coming out of a long curve strikes a pile of debris on the tracks. As a result, three crewmembers and four passengers are injured. Additional losses include $10 million in equipment and $200,000 in track-related damages. It is determined that a rock slide had occurred above a county roadway that runs parallel to the railway, about 50 feet higher on the side of the hill. The rockslide restrictive systems – systems designed to protect the roadway and subsequently the railway – had been in place in the area for some time.

The direct relationship or dependency related to the cause would likely be "physical" with the threat being an act of nature. Furthermore, this incident occurs in an area where rockslides are frequent and, historically, the restrictive systems installed have been successful in stopping significant debris from falling onto the road or the tracks below. In this instance, there also exists a dependency on the public works or highway departments of the county, which is not a typical part of the railway CI subsector.



Typical train tracks where debris could fall onto the rails (*Source:* Mathews, 2018).

A further investigation reveals that the restrictive systems have been removed deliberately in that one area without permits and without the landowner's knowledge. The county public works department states in the subsequent after-action report (AAR), that it depends on the county's law enforcement agency, in addition to its own observations, to detect illegal actions – like the system removal – during their regular patrols. In this hypothetical case, the railway also depends on the local law enforcement agency to detect malicious or deliberate illegal activity. The passenger rail company states its dependency on the local government's public works department and, in turn, that department is dependent on the local law enforcement agency. With such interdependencies in place, the resulting chain-of-events are termed "cascading effects."

Furthermore, the track is closed for the time required for inspecting and repairing it satisfactorily. The passengers traveling on the train that derailed do not arrive at their intended destinations on schedule. Some passengers likely have a critical need to arrive at their destinations on time. For example, perhaps someone does not make a critical meeting, so others then make an uninformed decision that, in turn, leads to additional negative consequences.

Assume that an extremist group deliberately caused the hypothetical incident described above as well as several other derailments occurring at about the same time across the country. In addition to the direct losses related to each incident, other consequences should be expected, for example:

- The passenger rail system could shut down temporarily across the nation to facilitate inspections;
- Freight rail systems could be impacted;
- The traveling public's faith and trust in the nation's rail passenger systems could take some time to return;
- The passenger rail company's cash flow could be affected; or
- The federal government may need to inject significantly more money to support the rail system.

Questions for Further Discussion

The above scenario is intended to facilitate thought and discussion about security, preparedness, and resilience for the nation's railways and in its passenger rail systems. Questions for discussion include:

- How should emergency preparedness and response professionals think about critical infrastructure protection?
- What are the first-, second-, and third-order effects that could happen should an incident occur?
- How reliable are these second- and third-order dependencies?

Although the railway incident used as the example was hypothetical, an actual derailment with similar losses did occur in October 2015. The National Transportation Safety Board determined the incident to be a simple "accident." Through no fault of the rail line or its personnel, the train struck a pile of debris that fell onto a track because of a rockslide.

The National Infrastructure Protection Plan of 2006 pointed out the importance of identifying and understanding cross-sector dependencies and interdependencies. Studies of catastrophic events since then are illustrative of this point. Not only do the rail systems depend on other sectors for much of their resilience, the loss or disruption of rail service from any hazard could have a cascading impact on other sectors, communities, and industry. Careful thought and consideration of interdependencies should be an essential element of any resilience planning.

Rick C. Mathews is a principal in the Mathews Group LLC and serves as a public service professor in the Rockefeller College of Public Affairs and Policy as well as in the College of Emergency Preparedness, Homeland Security and Cybersecurity, both at the at the University at Albany SUNY. He has over 40 years of experience in the areas of safety, security, counter-terrorism, and emergency preparedness. He has trained emergency responders across the nation and has conducted research in emergency preparedness, homeland security, and critical infrastructure interdependencies. He serves as a consultant to both public and private sector clients, the media, and emergency responder agencies.

MPAs & Disasters

With so many graduate degrees available, it can sometimes be confusing to know which to pursue when entering the world of emergency and disaster preparedness and response. DomPrep Advisor Andrew Roszak addressed one broad-based degree that covers many areas critical for managing disasters. In this podcast, Dr. Randolf Burnside of Southern Illinois University's Political Science Department and Dr. Anirudh Ruhil of Ohio University's Voinovich School of Leadership and Public Affairs share their insight about the Master's of Public Administration (MPA) degree and how it can help prepare professionals for jobs in both the public and private sectors.

Click to listen.

Andrew Roszak, Moderator, *Senior Director for Emergency Preparedness, Child Care Aware® of America*

Randolph Burnside, *Associate Professor at Southern Illinois University – Carbondale*

Anirudh Ruhil *Professor at Ohio University*

Historical Argument for Hardening Facilities

By Michael E. Gray

People's lives were changed forever on Tuesday, 11 September 2001. At the time of the 9/11 attacks, airport security was primarily focused on threats from guns and explosives. There was little worry about knives or sharp instruments. Even when detected at checkpoints, they were not often considered dangerous. Closing this security loophole came after these attacks, which spurred drastic security changes at all phases of the transportation system. However, this was not the first time such security has come into question. An historical review of terrorist tactics emphasizes the need to remain vigilant.

Airport security began in November 1955 after the incident on United Airlines Flight 629 from Denver, Colorado, to Portland, Oregon. The flight exploded just after takeoff with no survivors among the 44 people aboard. The investigation revealed that a bomb was placed in the checked luggage of a passenger, his mother Daisie E. King. Jack Gilbert Graham confessed to placing the dynamite in his mother's luggage to collect on her life insurance policy worth $37,500. In 1961, the Federal Aviation Administration (FAA) allowed armed guards on flights, but only if requested by the airlines or the Federal Bureau of Investigation. In the 1970s, the FAA became more security conscious after numerous hijackings. For example, in 1971, the FAA started screening passengers and carry-on luggage and using x-ray scanners. As security measures have changed, terrorist tactics have evolved.

Evolution of Terrorist Tactics

Six key examples demonstrate the evolution of terrorist tactics and need to adopt new security efforts. First, Ramzi Yousef was the bomb maker for the 26 February 1993 World Trade Center bombing and the master planner in the Bojinka 1994-1995 plot, which contained a number of phases: (1) assassinate the Pope on his visit to the Philippines; and (2) crash a small plane into the Central Intelligence Agency headquarters in Langley, Virginia. In December 1994, he assembled a bomb in the lavatory of Philippine Airlines Flight 434, set the timer to detonate four hours later, and placed the bomb in the lifejacket pocket under seat 26K near the fuselage (one fatality). This incident resulted in increased screening procedures for liquid explosives.

Second, in 2006, a transatlantic aircraft terrorist plot involved the detonation of liquid explosives disguised as soft drinks, which would be carried on board airliners travelling from the United Kingdom to the United States and Canada. Subsequent security efforts to restrict liquids were put in place after the plot was disrupted. Although some of these security measures were relaxed in the following months, carrying large containers of liquids onto aircraft is still currently prohibited.

Third, on 22 March 2016, three explosions occurred in Belgium's capital city of Brussels, with two at Brussels Airport (Zaventem) and a third at the city's Maalbeek metro station. The attack occurred outside the check-in area of the airport ticket counter. The attackers concealed the improvised explosive devices (IEDs), which consisted of a mixture of triacetone triperoxide (TATP) and ammonium nitrate, in large pieces of luggage. The bombs also consisted of screws and bolts for shrapnel. In response to the Brussels attack, the U.S. Senate approved legislation with a 95-3 vote that would boost domestic travel security by: increasing the number of bomb-sniffing dogs; strengthening employee vetting; increasing security at check-in and baggage claim areas; authorizing spending for FAA operations, airport improvements, and aviation research and development; and requiring new policy standards for commercial drones.

Fourth, in Turkey, an attack at the Istanbul Airport on 28 June 2016 occurred, with three suicide bombers armed with assault rifles opening fire both inside and outside the international terminal before detonating the explosives. The attack happened before the terrorists reached the ticket counter and security checkpoints. As a result, security was increased at airports around the world.

Past incidents have exposed security gaps, but terrorist tactics keep evolving. A look through history emphasizes the need to be forward thinking.

Fifth, on 6 January 2017, Esteban Ruiz Santiago arrived at the Fort Lauderdale-Hollywood International Airport after traveling on a Delta flight from Anchorage, Alaska, with a layover in Minneapolis, Minnesota. In Alaska, he checked a semi-automatic handgun with the Transportation Security Administration (TSA) according to the proper security protocol, without drawing attention to himself. After landing, he retrieved that handgun from baggage claim, loaded the weapon in the bathroom, and opened fire in Terminal 2 of the Fort Lauderdale airport. This loophole still requires some type of security procedure to be put in place to avoid similar incidents.

Sixth, in July 2017, Australia disrupted a sophisticated plot directed by the Islamic State group (IS). IS operatives shipped bomb components through international air cargo to Australia, then provided the recipients with directions how to assemble an IED. There were at least two planned attacks. The suspects first built an IED that was intended to blow up an airliner, and then allegedly attempted to build a chemical dispersion weapon. The latter device was apparently only in the beginning stages of development. On 3 August 2017, Australian Federal Police Deputy Commissioner Michael Phelan stated in a press hearing that the alleged would-be terrorists attempted "to place an IED on an Etihad flight out of

Sydney on the 15th of July." At no stage did the IED breach airline security, but it was one of the most sophisticated plots ever attempted on Australian soil. Numerous counterterrorism raids were conducted, with four people arrested and bomb-making material recovered. Enhanced security measures were implemented at airports.

A Move Toward Softer Targets

As access to air transportation has hardened, terrorists have shifted their attempts toward less secure transportation routes and venues that house large-scale events, such as sport stadiums and concert halls. For example, on 13 November 2016, a coordinated series of gun and suicide bomber attacks occurred in Paris, the first of which was an explosion at the Stade de France. A man wearing a suicide belt was reportedly prevented from entering the Stade de France after a routine security check detected the explosives. The man backed away from security guards and detonated the explosives outside the stadium. Target hardening at this access point prevented a mass casuality event (only one fatality in addition to the bomber). The concert hall and restaurants had more victims – in all, 130 fatalities and more than 100 critically injured.

Terrorists have demonstrated throughout history that they will change their tactics as security measures are implemented to close related gaps. Hardening of the air travel system will push terrorists toward softer targets like sport stadiums and music venues. Some vulnerabilities have been highlighted above – some addressed and others still require a response to address security gaps. However, knowing that terrorists will continually adapt to new security measures, it is necessary for preparedness professionals to "think outside the box" and be more proactive, rather than reactive.

Recommendations

When considering potential security gaps and solutions, consider the following recommendations:

- Extend the security perimeter to include parking areas (e.g., scan vehicles before entering airport parking or pickup and drop-off areas)
- Be more proactive than reactive (e.g., for some incidents, warning signs were witnessed but not reported or acted upon before attack)
- Increase security at the end of events
- Use more K-9 bomb-sniffing dogs
- Increase security cameras and monitoring
- Use behavior analysis
- Use vehicle X-ray machines at the entrance to parking areas
- Locate parking away from the venue, and use shuttle buses to transport fans to the stadium entrances
- Promote the "See something, say something" message
- Always be aware of surroundings (e.g., do not get distracted with cellphones and other technology)
- Be aware of new terrorist tactics (e.g., using vehicles to ram crowds)
- Before an event, extend the perimeter outward to include parking areas and transportation areas (e.g., some events no longer allow tailgating)

The time of getting to the airport half an hour before a flight and still making it, or using another person's ticket is over. However, hardening access to passenger areas at airports has led terrorists to evolve their tactics to attack areas outside security perimeters or shift their attention to softer targets. All modes of transportation – including rail and buses – as well as soft targets such as music halls and sports arenas need to be protected from tactics used in the past as well as those yet to be imagined.

On 9/11, at the time of the North Tower crash, the author was exiting the subway at the Chamber Street stop and observed the incident. At the time the Twin Towers collapsed, he was returning from taking an injured civilian to a triage area a block away. All he saw during the collapse was a wall of smoke and debris coming at him "like a big wave at the beach." He took cover under a parked truck. Living through 9/11 spurred his interest in developing counterterrorism strategies.

Michael E. Gray, adjunct faculty at SUNY Maritime, GBAT Department, Counter-Terrorism, Safety Security. SUNY Maritime has established a Masters Degree Tract/Certificate Program in International Transportation Security, which looks at all phases of global transportation security. He can be reached at mgray@sunymaritime.edu

Our commitment to BioDefense

has allowed us to be ready

for the Ebola outbreak

in West Africa.

Now, with the FilmArray system

and our reliable BioThreat Panel,

we are able to test for 16

of the worlds deadly

biothreat pathogens

all in an hour.

Now That's Innovation!

BIOFIRE®

DEFENSE

Learn more at www.BioFireDefense.com