

CBRNE



**Emerging Trends in
CBRN Detection - Moving Forward**
By Glen Rudner, Fire/HazMat

A Primer on PPE Training for Tactical Officers
By Richard Schoeberl, Law Enforcement

**The EMS Role on FAST Teams
And HazMat Assignments**
By Joseph Cahill, EMS

**TOPOFF 4 & Looking Glass RDD
Lessons Learned Exercises**
By Brandy Jones, Exercises

**Nuclear Smuggling: Detection
Challenges & Hasty Acquisition**
By Joseph Trindal, Law Enforcement

**NIMS-ICS & the Private Sector -
Good Fit, or a Stretch?**
By Steven Grainer, Fire/HazMat

**DomPrep Survey
DHS PS-Prep Program...Raising Awareness**
Prepared by Albert Romano, Senior Vice President,
Homeland Security, Michael Baker Jr. Inc.; Supported
by Dennis Schrader, President, DRS International, DP40

**Resilience: Developing Professionalism,
Clarifying the Incentives**
By Dennis R. Schrader, CIP-R

**How Clean is Clean?
Pre-Disaster Recovery Planning:
A New Focus on Deficiencies**
By Jordan Nelms, Viewpoint

**Gauging the Threat of an
Electromagnetic Pulse (EMP) Attack**
By Scott Stewart & Nathan Hughues, Viewpoint

Louisiana, Alabama, New Jersey, & Washington
By Adam McLaughlin, State Homeland News

The Next Generation of Dry Decon

- Wipe Away Bulk Chemicals
- Effective Dry Decon of Persons, Weapons & Sensitive Equipment
- Absorbs & Adsorbs Toxic Materials
- Indefinite Shelf Life
- Patented Three-Layer Design



Heat-Activated Personal Cooling

- Easy to Use & Maintain
- Recharges at Room Temperature Without Ice, Water or Refrigeration
- Non-Toxic & Non-Flammable
- Safer than Ice Vests
- Lightweight & Comfortable

Mass Casualty Evacuation

- Bus-Stretcher Conversion Kit
- Integrates with Most Buses
- Free-Standing Capability
- Low Maintenance Costs
- Long Shelf Life
- Accommodates NATO Stretchers
- Non-Ambulatory Transport



Editor's Notes

By James D. Hessman, Editor in Chief



The CBRN (chemical, biological, radiological, nuclear) threat to the United States has grown immensely in recent years, and is now a clear and present danger to all Americans, and to every aspect of the nation's political and economic well being.

That is the thrust of several reports and analyses commissioned for this special "roundup" issue of *DPJ*, which features: (a) A clear-sighted summary by Glen Rudner of the dangers and fiscal as well as operational difficulties in coping with CBRN threats or actual incidents; (b) A well articulated report by Joseph Trindal on the perhaps impossible task of screening almost every shipping container entering the United States – 1,400 radiation portable monitors distributed among 500 ports of entry – for evidence of nuclear radiation or other hidden dangers; (c) A review, by Jordan Nelms, of the frustratingly inconclusive investigation of the September 2001 anthrax attacks – which in expanded form could have killed many more Americans than died in the much better publicized 9/11 passenger-aircraft attacks on New York City and the Pentagon; and (d) An update, by Brandy Jones, on the lessons learned from the multi-jurisdictional TOPOFF (Top Officials) 4 "dirty bomb" exercise in New Jersey.

DPJ readers are urged to read all four of those articles, then shift to the latest "DP40" Survey – by Albert V. Romano – on the DS-Prep (Private Sector Preparedness) program. Congress has mandated that DHS establish a full spectrum of programs and initiatives that would help persuade the nation's businesses and private-sector organizations to play a major role in making their own communities, and the nation as a whole, better equipped to prevent, prepare for, and, if necessary, respond to and recover from not only CBRN attacks but also a broad spectrum of other dangers and disasters ranging from hurricanes and floods to pandemics and so-called "agro-terrorist" outbreaks. So far, very little has been done in any of these areas – partly because of inadequate funding, but also, it seems apparent, from a lack of enthusiasm. The DHS bureaucracy and the American people are equally to blame for the latter.

Two other articles complement the Survey: (1) an update by Steven Grainer on the NIMS (National Incident Management System) and ICS (Incident Command System) programs – and the importance of mutual-aid agreements in the implementation of both. (2) A reprint, from Stratfor Global Intelligence, of an article by Scott Stewart and Nathan Hughes on the crippling effects of an EMP (electronic magnetic pulse) attack on the United States – which could immediately shut down almost all electronics equipment and devices of all types ranging from radar tracking systems to emergency warning networks to radio and television stations. EMP attacks are one of the oldest and most complicated "present dangers" known to the nation's political and military readers, and nuclear scientists, but not to the American public at large.

In addition: Richard Schoeberl reports on the proper design, fit, and use of Personal Protective Equipment; Joseph Cahill discusses the "two-in/two-out" rule used to magnify the effectiveness of community-based Firefighter Assistance and Search Teams; Dennis Schrader comments on the increasing importance of "Resilience" – particularly as spelled out in the 2010 Quadrennial Homeland Security Review and the 2010 Bottom-Up Review; and Adam McLaughlin rounds out the issue with updates on recent noteworthy preparedness events in Alabama, Louisiana, New Jersey, and Washington.

About the Cover: The international bio-hazard symbol provides an appropriately menacing red-for-danger background for three of the most effective anti-CBRN systems and devices now available: Idaho Technology's RAZOR EX system, which uses sensitive cutting-edge technology to detect and identify Bio Threat agents; Bruker Detection's Raid M100, used to detect, classify, and quantify toxic industrial chemicals and chemical-warfare agents; and Avon Protection's C50 Mask, which is specifically designed to improve integration with equipment for tactical operations. (Composite image by Susan Collins.)

Business Office

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

Staff

Martin Masiuk
Publisher
mmasiuk@domprep.com

James D. Hessman
Editor in Chief
JamesD@domprep.com

John Morton
Strategic Advisor
jmorton@domprep.com

Susan Collins
Creative Director
scollins@domprep.com

Catherine Feinman
Customer Service Representative
cfeinman@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

Advertisers in This Issue:

AVON Protection

Bruker Detection

Environics

Emergency Preparedness & HazMat
Response Conference

First Line Technology

IAEM 58th Annual Conference & EMEX
2010

ICx Technologies

Idaho Technology Inc.

Southeast Counter-Terrorism & Emergency
Response Conference

Meridian Medical Technologies™

QuickSilver Analytics

PROENGINE Inc.

Upp Technology Inc.

WL Gore & Associates

© Copyright 2010, by IMR Group, Inc.; reproduction of any part of this publication without express written permission is strictly prohibited.

DomPrep Journal is electronically delivered by the IMR Group, Inc., 517 Benfield Road, Suite 303, Severna Park, MD 21146, USA; phone: 410-518-6900; fax: 410-518-6020; 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 its use or interpretation.

IMR GROUP



BREATHE EASY.

The Extended Response Team (XRT) suit provides the ultimate combination of protection and mission time.

Equip your team with confidence and enhanced response capability from the trusted leader in protective fabrics. The quick-donning XRT suit gets your team to operations sooner with its one-piece design that requires no additional taping. Breathable GORE® CHEMPAK® Selectively Permeable Fabric reduces heat and moisture buildup, allowing your team to stay on the scene for up to eight hours. Certified to the NFPA 1994, Class 3 standard, the single-mission XRT suit is the preferred choice for perimeter response.

Visit our website for more information on the new XRT suit and other suits using W. L. Gore & Associates' innovative fabrics.

THE NEW XRT SUIT – AVAILABLE NOW.

www.GoreChempak.com/XRT

W. L. GORE & ASSOCIATES, INC.

Technical Fabrics

800.431.GORE (4673)



Chempak®

FABRICS

CHEMPAK, GORE and designs are trademarks of W. L. Gore & Associates ©2010 W. L. Gore & Associates, Inc. Warning: No products, including garments, footwear or handwear, offer absolute protection, even when new, and their protective performance will decline with wear, tear, abrasion, and other damage associated with use.

Contributors

First Responders

Kay Goss
Emergency Management

Joseph Cahill
EMS

Glen Rudner
Fire/HazMat

Steven Grainer
Fire/HazMat

Rob Schnepf
Fire/HazMat

Joseph Trindal
Law Enforcement

Rodrigo (Roddy) Moscoso
Law Enforcement

Joseph Watson
Law Enforcement

Medical Response

Michael Allswede
Public Health

Raphael Barishansky
Public Health

Bruce Clements
Public Health

Theodore (Ted) Tully
Health Systems

Adam Montella
Health Systems

Government

Corey Ranslem
Coast Guard

Dennis Schrader
DRS International LLC

Adam McLaughlin
State Homeland News

Infrastructure

Neil Livingstone
ExecutiveAction

Industry

Diana Hopkins
Standards

Emerging Trends in CBRN Detection – Moving Forward

By *Glen D. Rudner, Fire/HazMat*



The United States is a target-rich environment for CBRN (chemical, biological, radiological, and/or nuclear) terrorism. There is a compelling need, therefore, for a strategy that takes into account the efforts already taken and provides an overarching framework to enhance the nation's first-responder abilities to detect and prevent future CBRN incidents.

There are already many individual and collaborative efforts going on that should contribute constructively to the development of more advanced anti-CBRN technologies and equipment. The first step in the process to meet current and future needs, it seems reasonable to say, is to develop an overall picture of current and future development scenarios. The U.S. Department of Homeland Security (DHS) and industry stakeholders should then expand and evaluate the development timeline and agree on a strategic process for implementation. Fortunately, significant research in analyzing and improving technological capabilities has been carried out in a number of fields – including but not limited to the following: mass spectrometry, ion mobility spectroscopy (IMS), infrared (IR) spectroscopy, Raman spectroscopy, polymerase chain reaction (PCR), dose meters, Geiger-Muller detectors, and scintillation detectors.

The developers of today's advanced-technology detection systems are trying to improve both their functionality (improved sensitivity as well as greater selectivity) and their performance (particularly their portability). In today's environment of heightened security, governments are investigating numerous ways to ensure the safety of their citizens. DHS, along with other U.S. public agencies and private-sector organizations – e.g., government/private laboratories, academic institutions, and private-sector businesses – are working to develop even more advanced and innovative CBRN technologies through programs funded by numerous organizations and agencies. The new high-tech systems now emerging are expected to provide more accurate and precise information to emergency responders so that they may take appropriate action both before an incident occurs and after the release – either deliberate or intentional – of CBRN agents.

Current trends in the industry are focused on developing technology for detection instruments that will be characterized by improved sensitivity and selectivity, a broader detection range, a more rapid monitoring speed, a real-time detection capability, and reduced false-alarm rates. The instrumentation platform itself should ideally be compact, lightweight, portable, and flexible. Additional technological advances – e.g., the use of semiconductor integrated circuit (IC), telecommunications, networking, and information systems – will undoubtedly add significantly to the development of even more advanced CBRN detection systems.

Significant Progress – But a Long, Hard Road Ahead

As today’s highly charged, technology-driven world moves forward, it can be safely assumed that there will be even greater advances within the foreseeable future.

The introduction of wireless sensor networks, for example, and the development, production, and use of more sophisticated modeling and simulation tools should be of immense help to emergency responders – and to those involved in the decision making process. Several years ago the introduction of “bio-watch” systems to major metropolitan areas proved that stand-off biological perimeter monitoring systems and devices can work – to a certain extent. However, the precision, accuracy, specificity, and selectivity of such systems are still somewhat short of what is required, which means that additional upgrades and refinements are still needed in this field. There is a similar need to develop, test, and install highly capable chemical and radiological detection systems and devices.

Several government agencies, and private-sector companies and corporations, already are researching the possibility of developing, building, and installing detection systems that can view several types of CBRN agents at the same time to provide an early warning of each and all of those threats – and there has been impressive progress in several closely related research and development (R&D) efforts. Nonetheless, it also has become apparent that there is a parallel need, to ensure optimum use, to identify the most suitable locations for deploying and installing these and other improved detectors.

As in the past, another issue likely to challenge developers is the building of portable, economical, lightweight, real-

time detectors characterized by low power consumption – in a long-term detection mode – while also facilitating user dexterity. Another important factor to consider is that most if not all current government-funded R&D programs in CBRN are in the chemical and biological detection fields; these efforts should be augmented and/or replicated in the radiological and nuclear detection fields as well.

The first step in the process to meet current and future needs, it seems reasonable to say, is to develop an overall picture of current and future development scenarios; the Department of Homeland Security and industry stakeholders should then expand and evaluate the development timeline and agree on a strategic process for implementation

As the industry moves forward in the development of CBRN detection equipment, it will be extremely difficult to maintain its focus on the current threats now facing the nation’s responder community. There are, however, many emerging trends that provide an insight into various encouraging development initiatives around the globe in CBRN detection technologies, current development scenarios, adoption factors, and technological development strengths – and, of at least equal but perhaps greater importance, some gaps and shortfalls as well. A dispassionate analysis of the still growing number of terrorist attacks that have occurred and are continuing to occur around the world should demonstrate that the United States is still not immune from many of the major CBRN threats now facing the nation – and may never be. For

that reason alone, there must be not merely continued, but increased, concern over chemical, biological, radiological, and nuclear (CBRN) terrorism.

Glen D. Rudner is a project manager for CRA-USA, where he works with senior management executives on major corporate issues; he is currently assigned to management of the Target Capabilities List project for the U.S. Department of Homeland Security. A recently retired Northern Virginia Regional Hazardous Materials Officer; he has been heavily involved during the past 32 years in the development, management, and delivery of numerous local, state, federal, and international programs for such organizations as the National Fire Academy, the FBI, and the Defense Threat Reduction Agency.

A Primer on PPE Training for Tactical Officers

By Richard Schoeberl, Law Enforcement



Law enforcement and intelligence agencies face myriad challenges in their efforts to combat terrorist organizations. Recent acts, and attempted acts, of terrorism, Congressional reports on “failed readiness” capabilities, and

the Department of Justice’s concern over the nation’s ability to respond to Weapons of Mass Destruction (WMDs) all indicate that the United States is not yet fully prepared for a chemical, biological, radiological, nuclear, and/or explosives (CBRNE) attack. Moreover, although recent intelligence reports indicate that al Qaeda’s infrastructure is weakening, its efforts to acquire WMDs have not – and neither has its intentions to use such weapons against the United States and its allies. The continued efforts of terrorist organizations to acquire one or more CBRNE weapons means that the United States cannot afford to be unprepared. In short, being prepared is no longer just an option – it is a very high priority.

Although there are many factors contributing to the current lack of U.S. preparedness, inadequate training should not be one of them. As a community, U.S. first-responder agencies cannot afford to train only 10 percent of the time to deal with a theoretical “10-percent chance” that a CBRNE incident will occur. Often, the question of why al Qaeda has not yet attacked the United States again – as it has done overseas in smaller-scaled and isolated incidents – perplexes almost all of the experts in this field. Many of them have in fact suggested that al Qaeda is planning an attack that would be both lethal and spectacular. If intelligence agencies give any credence to the information gathered over the past several years, they would also certainly agree that a CBRNE attack may be looming just over the horizon.

Knowing that the storm is approaching, but not knowing when and where it will strike, is an unfortunate reality that law enforcement agencies have learned to accept. Those agencies know that they must be ready, prepared, and equipped to deal with any and all facets of an attack, particularly and specifically a CBRNE attack. For the tactical operator, moreover, preparing for a CBRNE attack goes far beyond intelligence gathering. Once the unknown becomes known, agencies must have people in place who are equipped to deal not only with the situation at hand, but also prepared mentally, physiologically, and tactically.

Life, Death, and the Risk of Infection

For a tactical officer, it is particularly critical – of literally life-or-death importance – to know how PPE (Personal Protective Equipment) clothing works and how wearing it affects the body. Sometimes the risk of infection from a CBRNE attack may be relatively small, but the effects and health consequences associated with it might still be extremely severe. Because PPE is not designed to do anything other than what it was originally intended to do – i.e., protect the wearer – it must be well maintained, in strict accordance with manufacturer recommendations, so that it works when needed.

When concerned with hazardous materials such as a chemical, biological, radiological, or nuclear (CBRN) device or even a clandestine drug laboratory, the responders’ first enemy is contamination. To cope with that specific danger, SWAT (special weapons and tactics) personnel protect themselves by donning coveralls, gloves, masks, chemical protective clothing, and respirators. Wearing the correct level of protective clothing is of vital importance, and for that reason PPE equipment should be selected based on the known properties of the specific hazard.

Unfortunately, of the many factors that must be considered when beginning a dangerous operation, the specific hazards likely to be encountered are usually unknown to the tactical operator. Because of the unique characteristics of each situation, therefore, tactical officers dealing with a CBRNE attack must be prepared at all times for the ultimate challenge – engaging a hostile subject who is equipped with a CBRN weapon or device. When the hazard is known to be relatively minor – sometimes just a simple nuisance – minimal protection is perhaps all that may be required. However, when conditions are unknown, tactical teams should always use the greatest level of skin, respiratory, and eye protection – collectively known as “Level A Protection.”

U.S. responder agencies themselves, at all levels of government, should be assigned the responsibility (and given the resources needed) for: (a) outfitting tactical officers with the proper levels of PPE clothing and gear; and (b) providing adequate training – and training time. Because all or almost all PPE clothing is much more cumbersome than the typical uniform worn by a tactical officer, team members should be provided ample training in equipment preparation as well as in the performance of specific tasks while actually wearing the PPE clothing. Today, most federal law enforcement officers are accustomed

to wearing suits to work. Nonetheless, they must be prepared to change, at a moment's notice, from a Brooks Brothers suit into SWAT tactical gear and outfitted PPE. Moreover, while wearing a tactical vest, web gear, and duty belt on top of the PPE, the officer must be confident that those items will not compromise the integrity of the PPE suit. The ability to maneuver and to address the task at hand is the ultimate goal – and effective training is the only way to ensure that that goal is achieved.

Time, Trips, Slips, and Other Hazards

Not incidentally, individuals wearing PPE must be concerned not only with the hazardous agents they may face but also with issues – heat stress, for example – that in other circumstances might safely be overlooked or ignored. Moreover, military and civilian users must develop and use “best estimates” of an acceptable operation time for wearing PPE that will avoid excessive heat stress – which could threaten their ability to function as well as their health and safety. Current approaches to determining operation time tend, understandably, to be conservative and err on the side of caution. Such conservative estimates may therefore require a responder to prematurely cease his or her work efforts and remove the PPE. At the same time, care must be taken to avoid an overly aggressive approach that overestimates operation time and could threaten the health and safety of responders or others. Proper training will, or should, familiarize operators with the limitations associated with operation time.

Being a tactical operator is a dangerous occupation in itself; and it is impossible to work in a hazardous CBRN condition without donning PPE. Although most recorded injuries result from innumerable factors – e.g., trips, slips, falls, hostile engagement – wearing PPE can add the hazard of heat stress to the equation. Heat stress can and does occur most often when the PPE interferes with the body's own built-in ability to cool itself. In most if not quite all operational situations, tactical teams do not face the hazard of heat stress, but they still must be aware of the danger. When members are sealed up in protective clothing, the body cannot cool itself properly. The longer that situation persists, the higher the body temperature rises until the body eventually succumbs to heat stress. If the same conditions persist and the body can no longer cool itself, heat stress can evolve to heat stroke.

Heat stress and fatigue are important factors – especially in situations in which quick judgments are necessary. Tactical operators rely on their training, skill sets, and judgment; when these factors become impaired, poor decision making can

quickly follow. It is highly recommended, therefore, that tactical officers routinely wearing PPE obtain medical clearance by reporting for regular physicals. It is also important that tactical teams regularly address such closely related factors as medical readiness, physical fitness requirements, on-scene rehabilitation, and hydration strategies.

The Three Essentials: Teamwork, Training & Temperature Awareness

The use of PPE and insistence on medical monitoring are obviously important for the individual officer's own safety as well as the safety of the entire tactical team. All persons serving on a team are individually and collectively both crucial and integral to the team's success. If the individual fails, the team fails. Furthermore, wearing the wrong equipment, or ill-fitted equipment – or even the right equipment, worn improperly – can have fatal consequences for the entire tactical team – and for their mission. It is important that tactical team members understand not only the benefits but also the limitations of their PPE.

The importance of training cannot be overemphasized – the operator and the team must understand the potential limitations associated with PPE. Operators will know through adequate training that PPE requires a specific amount of time to put on, and should therefore make adjustments as needed to allow for that time during an operation. Through adequate and effective training, operators gain understanding of the limited dexterity and impaired mobility they may, and probably will, experience while wearing PPE. Many, but not all, will probably have difficulty dealing with the impaired communication and reduced vision associated with PPE. In addition, most – again, if not all – operators will have difficulty dealing with the psychological stress, use limitations, dwindling oxygen availability, increased weight, and heat stress associated with their PPE.

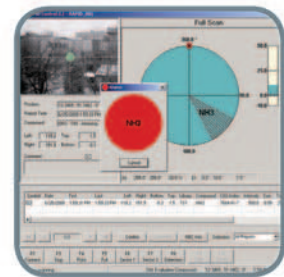
Numerous studies have shown that working in a high-temperature environment creates greater physiological and psychological strain than performing the same work in a neutral environment. Most chemical protective outfits are both heavy and cumbersome; for that reason alone, wearing PPE both decreases the body's ability to deal with stressors and restricts freedom of movement. It is important, therefore, to become accustomed to the limitations and physical demands that PPE places on the operator, but that can be accomplished only through adequate training.

The optimum way for the human body to combat heat stress is to allow the body to cool normally – i.e., through evaporation. But that is not possible while wearing PPE or other

RAPID

Stand-off Detector for Atmospheric Pollutants

- For the remote detection of atmospheric pollutants and chemical warfare agents
- Allows for measurements in the spectral wavelength range from 14 μm to 8 μm
- Four libraries of chemical compounds, can detect up to several kilometers line-of-sight



+1 (978) 663-3660 x 1418 • nbc-sales@bdal.com • www.bruker.com/detection

think forward

CBRNE Detection

“non-breathable” clothing in which the body temperature can rise both rapidly and unexpectedly. Because each operational situation is unique in at least some respects, tactical teams are not afforded the luxury of taking a break during an operation. More specifically, tactical officers cannot, particularly in “the hot zone,” afford to remove equipment due to extreme heat and therefore must remain hydrated without compromising the integrity of their PPE.

Tactical operators can expect large volumes of sweat loss during tactical operations due to: (a) their strenuous work; (b) the usually extreme heat conditions encountered; and (c) the impermeability of the PPE materials. During taxing work in a hot environment, or while wearing impermeable clothing, a typical adult human might lose more than two quarts of sweat per hour. It is common, therefore, for tactical operators to lose even more sweat per hour when working in hot temperatures while fully PPE-outfitted. That sweat loss contributes significantly to a decrease in plasma volume, imposes additional strain on the cardiovascular system, and decreases thermal tolerance. Tactical operations usually involve performing strenuous activity in a hot and aggressive environment while wearing restrictive and heavy PPE – and that combination of circumstances makes tactical operators more susceptible to heat stress.

Deadly Combinations & A Two-Team Approach to Survival

Heat stress and the resulting increase in body temperature have innumerable, and almost always harmful, effects on the human body – e.g., increased cardiovascular strain, dehydration, the rapid onset of muscular fatigue, and interference with cognitive functions. The inability to process information quickly, combined with physical fatigue, can be a deadly combination for tactical operators. Decision making capabilities deteriorate rapidly with extended exposure to heat stress – which has been shown to reduce the cognitive and mental-processing abilities essential to decisions involving both simple and complex tasks. The degree of decrements of these tasks is directly related to the deep body temperature, which is a function both of duration and of the time and intensity of heat exposure.

The best way, almost always, to treat heat stress is to address that potentially lethal problem before it happens. High temperatures and humidity caused by PPE stress the body’s ability to regulate and cool itself. Among the more obvious symptoms of heat stress are dizziness, cramping, nausea, severe headaches, hot and dry skin, and extreme body temperatures – as much as 106 degrees, and sometimes even higher. Knowing the symp-

toms, recognizing the limitations imposed, and preparing the wearer’s body – primarily through adequate training – can help significantly in reducing the chance of experiencing heat stress.

To reduce the harmful effects of both heat stress and fatigue, tactical teams should be prepared to outfit two or even three operational teams – which should be strategically positioned and prepared to rotate in an orderly sequence to address a “typical” hazmat situation. Rest cycles usually: (a) give the body an opportunity to rid itself of excess heat; (b) slow down the production of internal body heat; and (c) increase the body’s blood flow to the skin.

Tactical teams should focus on reducing the harmful effects of heat stress by, among other things, acclimating themselves ahead of time with the PPE they have been issued. Donning PPE equipment once or twice a year does not provide enough time to prepare operators with the specific knowledge they need to operate effectively. Operators should therefore: (1) allow their bodies to naturally and gradually acclimate to the equipment they are wearing; and (2) familiarize themselves, beforehand, with the specific limitations imposed by the equipment they will be wearing. Drinking plenty of water before, during, and after can limit the effects not only of the water loss itself but also of the weight loss caused by water evaporation during an operation. Operators also should avoid the excessive use of alcohol, not only because it can so easily lead to mental confusion but also because it causes dehydration – which imposes an added burden to the body during very high temperatures. One of the best protections against heat stress, of course, is overall physical fitness, which not only can improve an operator’s coordination and concentration but also increase his or her alertness, strength, and durability.

Once again, the best means of combating heat stress associated with tactical teams is addressing that adverse circumstance before it happens. An “operator down” due to heat stress can defeat the team’s overall mission – and endanger a large number of lives. Knowing individual limitations, addressing the problems caused by inadequate training, and taking the necessary precautionary measures to combat heat stress can make a major and frequently life-saving difference in the outcome of a CBRNE incident.

Richard Schoeberl has over 15 years of counterintelligence, terrorism, and security management experience gleaned from his career with the Federal Bureau of Investigation. His experience ranged from service as a field agent to leadership responsibilities in executive positions at FBI Headquarters and the National Counterterrorism Center. He worked a majority of his FBI career in the Counterterrorism Division providing oversight to the FBI’s international counterterrorism effort. Schoeberl held collateral duties as a certified FBI instructor and a member of the FBI SWAT program.

The EMS Role on FAST Teams & HazMat Assignments

By Joseph Cahill, EMS



Firefighter Assist and Search Teams (FASTs) are basically teams of responders positioned as an on-site “just in case” resource – suited, equipped, and ready to go into action on short or no notice – on a mission to “rescue the rescuer(s).” First responder duties – particularly in firefighting and/or on hazmat (hazardous materials) missions – are inherently dangerous, so there is always a chance on any response that the responders may suddenly find themselves in a life-threatening situation from which they are unable to extricate themselves. In short: Being a responder is about taking controlled risks to save the lives of others; however, *controlled* or not, it still entails some risks.

FAST teams are an outgrowth of the former fire-suppression teams and as a result were originally conceived of, more or less, as a fire-apparatus asset – similar in some ways to a ladder truck or engine, but with a crew to operate it, enter a burning building, and rescue any imperiled responders already inside the building.

The just-in-case concept, of course, can be and has been extended to other situations such as hazmat missions and police-unit tactical responses. Preferably, the members of FAST teams should possess the same skills as the responders who are already operating on scene. The principal reason for this guideline is that the skills and experience of responders should, if possible, reflect the specific type of hazard involved. Nonetheless, it is imperative that a FAST team of any type should be augmented with an on-site EMS (emergency medical services) resource.

Two In/Two Out – Plus Dedication & Control

One of the most important operational missions of a SWAT team, usually, is to rescue hostages. For that reason, every SWAT program should include training in the rescue and/or extrication of individual SWAT members themselves. By creating a dedicated “entry team” whose job it is to rescue responders who find themselves in an uncontrolled situation, command imposes a needed measure of control back over the incident.

Within the overall hazmat community the usual standard is “two in, two out” – in other words, two responders in protective gear within the operation zone should be backed by a two-responder entry team suited up and ready to go into the zone to support the responders already there. That support is focused on: (a) rescuing the fallen, endangered, or otherwise imperiled hazmat operators inside; and (b) removing them to the outside of the hot or high-hazard zone.

At the edge of any scene is the interface between the scene’s operational area, or hot zone, on the one hand – and the rest of the world outside. On a hazmat scene this “warm” zone is usually where the rescued personnel are decontaminated and cleansed of any hazardous materials on themselves, their protective gear, and/or their equipment.

The Combined Stress Of Hostility & Excessive Heat

Any high-risk event requires having EMS personnel on-scene; to maximize their effectiveness, though, EMS personnel must be waiting and ready for any victim or patient who enters or is carried into the warm zone. Another planning consideration is that the protective gear that hazmat responders must wear into and at the scene of a hazmat incident – to separate them from the hostile chemicals – results in additional stresses, both of carrying the extra weight and enduring an excessive heat buildup.

Having EMS on-scene has one major compensating advantage, though: It allows for the rapid treatment of responders. An EMS component therefore should be considered an essential part of the FAST team responding to any hazmat incident and for that reason should be available only for the support of the responders on-scene; however, the members should be assigned to and serve in the decontamination area, rather than serving as part of the entry team.

Another important hazmat guideline is that any contaminated patient must be decontaminated *prior to receiving care* – otherwise, the contaminating chemical may well spread and come into further contact with the patient by and during the act of providing medical care. That precautionary rule applies even more to paramedic-level treatments – which are, in general, somewhat more invasive.

A final but essential point: Having the resources available to rescue and treat responders who themselves are in deadly peril because of their efforts to rescue others is not only a good practice within the response community itself; it is also an ethical imperative for their leaders.

Joseph Cahill, a medicolegal investigator for the Massachusetts Office of the Chief Medical Examiner, previously served as exercise and training coordinator for the Massachusetts Department of Public Health, and prior to that was an emergency planner in the Westchester County (N.Y.) Office of Emergency Management.

Biological Sampling

Fast, Reliable, Easy to Use

All-In-One Swab Kit



- Simple biological* sampling
- One time use
- Compatible with CRP HHA
- 2-year shelf life
- Sold in 5 packs
- Integrated into Quicksilver

CBRE Sampling Kits or
sold separately



For more information
www.qckslvr.com or 800.725.7587



TOPOFF 4 & Looking Glass RDD Lessons Learned Exercise

By Brandy Jones, Exercises

Communication is a key to success in disaster preparedness, as became apparent in the lessons learned from the full-scale TOPOFF 4 “Looking Glass” tabletop exercise (TTX) on 17-18 October 2007. The “TOPOFF” (Top Officials) participating in that exercise – fourth in the TOPOFF series – learned three particularly important communications lessons. First, states should involve private-sector companies fairly early in the preparation process, and at the outset of the emergency. Second, private companies should ensure that their own IT (information technology) resources are available for use in emergencies. Third, all states should develop and be ready to use their volunteer databases *before* an incident occurs, not during or after.

Thousands of federal, state, territorial, and local jurisdictions and agencies throughout the country participated in the numerous exercises and scenarios featured in TOPOFF 4. The New Jersey Business Force provided sponsorship of the Looking Glass TTX – an exercise within TOPOFF 4, which involved 26 jurisdictions, agencies, and businesses. (The full TOPOFF 4 after-action report is available on the *Lessons Learned Information Sharing* website (www.llis.gov), along with lessons learned and other information about this and other TOPOFF exercises.)

The detonation of a radiological dispersal device (RDD) in Jersey City, New Jersey – directly across the Hudson River from the Manhattan borough of New York City – was the “main event” in the Looking Glass TTX scenario. An RDD is a conventional explosive – also known as a “dirty bomb” – that, upon detonation, releases radioactive material into the surrounding area. Although it does not cause the type of catastrophic damage associated with a nuclear detonation, there are severe rescue, health, and long-term decontamination concerns associated with an RDD.

Looking Glass TTX participants found that the explosion would probably exhaust the state, county, and local government response resources immediately available. Largely due to that reason, private-sector representatives should be involved in the planning for such an incident to be available to assist the government agencies and organizations early on in the incident. Moreover, the private sector provides more and better resources to help in the response and recovery efforts. Regularly and routinely, agencies and organizations, at all levels of government, should exchange intelligence and information with the private sector prior to an incident.

Bridging the Gap, Advance Planning, Volunteer Databases

During the October 2007 exercise, participants relied on the private sector’s information systems to help bridge the gaps in responder capabilities by providing rapid resource utilizations, alerts, and warnings as well as strategic collaboration services. The participants also found that, during the first hour after the simulated RDD explosion, numerous information systems ran the risk of crashing because of either a communications surge or the explosion itself. To ensure that valuable private-sector assets are available in the future as and when needed, the TOPOFF-4 after-action report recommends that businesses ensure that preparations and plans are in place beforehand to deal with similar disruptions that might occur.

The exercise participants also found, not surprisingly, that using preregistered and prescreened volunteers during the exercise facilitated faster responses. While planning for an incident, emergency managers therefore should carefully consider making prior arrangements with organizations that already maintain volunteer databases – e.g., the American Red Cross and/or the World Cares Center. Such arrangements could help significantly to speed the deployment and mobilization of volunteers during a time when, literally, seconds count.

To briefly summarize: Whether communicating with private organizations before an incident, communicating with private organizations to ensure well-prepared disaster plans are readily available, or communicating with other groups to access volunteer databases, pre-planning for potential disasters is and will be a vital component of overall domestic preparedness. Learning from the experiences and exercises of similar groups can save not only time and money, but also lives.

To learn more about the RDD responses and/or the TOPOFF 4 Looking Glass TTX, to share your own experiences with exercises and plans, or to pull information from a wide range of other documents on similar subjects, visit Lessons Learned Information Sharing (LLIS.gov) at www.llis.gov. LLIS.gov is the national online network of lessons learned, best practices, and innovative ideas serving the nation’s emergency-management and homeland-security communities.

Brandy Jones is an outreach analyst for Lessons Learned Information Sharing (LLIS.gov), the Department of Homeland Security/Federal Emergency Management Agency’s national online network of lessons learned, best practices, and innovative ideas for the U.S. homeland security and emergency management communities.

Nuclear Smuggling: Detection Challenges & Hasty Acquisition

By Joseph Trindal, Law Enforcement



The detection, prevention, and combating of radiological and/or nuclear (rad/nuc) smuggling is a daunting responsibility. The United States has long led the world in protecting its own rad/nuc assets from theft, diversion, and attack. Protecting the U.S. homeland, though, from rad/nuc attacks – by terrorists and other non-state actors – is a relatively recent and more difficult mission. The Customs and Border Protection (CBP) branch of the Department of Homeland Security (DHS) leads the interagency effort in protecting U.S. borders. Despite considerable improvement in numerous operational areas since 11 September 2001, however, several difficult challenges remain, particularly in the detection of rad/nuc materials.

Recognizing the ease by which terrorists could use the global supply chain to introduce rad/nuc materials into the United States, Congress authorized DHS in 2005 to create the current Domestic Nuclear Detection Office (DNDO), which is responsible for providing agencies involved in the effort to combat rad/nuc smuggling with the latest technological solutions needed to carry out that mission. Early detection, of course, is an essential aspect of the DNDO's goal of building a "nuclear detection architecture" for combating rad/nuc smuggling.

For over 10 years, the primary radiological detection systems deployed in U.S. Ports of Entry (POEs) have been Radiation Portal Monitors (RPMs), installed in both fixed and portable configurations. According to DHS, CBP now deploys an estimated 1,400 RPMs at over 300 POEs. The United States has long recognized the potential rad/nuc threat posed by the easy availability, in hundreds of ports throughout the world, of international shipping containers, which for decades have been used for the smuggling of illegal immigrants, weapons, drugs, and other illicit materials. (DHS recently reported, though, that nearly, but not quite, 100 percent of the shipping containers entering the United States are now being screened.)

Shielding Limitations and Other Factors

Widely used RPM technology is much less effective, however, at detecting radiological materials that are "shielded" in one way or another. CBP uses RPM detection as a primary screening method for vehicles and containers entering the United States through POEs. When an RPM alarm activates, the vehicle becomes subject to a secondary and more thorough screening inspection. Nonetheless, because of certain limitations of the RPM technologies predominantly used in primary screening, shielded rad/nuc materials could pass through that the POE screening would not detect.

Advanced radiographic imaging is fairly effective at detecting materials *density* – the measurement of which

may be indicative of shielded rad/nuc smuggling. For that reason, CBP and other agencies today make limited use of advanced radiography (and associated algorithms) to enhance the secondary screening process, but rarely use it as a primary screening measure.

Nonetheless, in 2005, DNDO began exploring – in its Cargo Advanced Automated Radiography System (CAARS) – the viability of expanding the development and use of advanced radiography. The CAARS initiative, which

carried an estimated \$1.5 billion price tag, was expected to enhance the CBP's primary screening processes, thereby at least partially closing (in theory) the gap in entry detection of heavily shielded rad/nuc materials.

Balancing Security and Commerce

Clearly, CBP's mission requires a constant balance between maintaining security and facilitating U.S. access to the global supply chain. The Government Accountability Office recently issued a statement for the record to the U.S. Senate Committee on Homeland Security and Governmental Affairs in which the GAO cited an apparent lack of interagency coordination and communication between





A single solution for all your needs



From emergency management, mass casualty evacuation and patient tracking to day-to-day asset, resource and inventory management, irms|360™ Enterprise is the only proven integrated management solution for statewide public health and public safety.

The irms|360 Enterprise application framework is designed to be scalable, interoperable and highly available, providing federal, state and local agencies a comprehensive solution suite for tracking critical supplies, people and processes.

Asset
Management

Clinic
Management

Emergency
Management

Patient
Management

Vaccine
Management

Warehouse
Management

DNDO and CBP over the viability, safety, and effectiveness of using CAARS technology for widespread rad/nuc primary screening.

At least partly as a result of CBP's objection that the CAARS program's advanced radiographic scanning might have an adverse impact on already overcrowded POE egress, DNDO decided in 2007 on a "course correction" that significantly scaled back the acquisition and deployment of advanced radiographic technologies.

Three years later, DNDO seems to be no closer to providing CBP with a viable solution for advanced radiographic imaging that balances the need for security with the efficient movement of vehicles and goods through the nation's ports.

A key requirement for CBP application in primary screening is swift and automatic detection. The CAARS solution promised, in theory, to meet that requirement. But it failed to do so – primarily because, as the GAO reported, the system's algorithm technology was and is not yet sufficiently developed. Apparently driven by a sense of deployment urgency, DNDO reportedly decided on continuing with an aggressive development and acquisition schedule that exceeded the capabilities of the automated algorithm functionality.

A Lack of Communication And Collaboration?

GAO also reported that DNDO failed to consult with users of this critical detection- enhancement technology both before and during the development and acquisition phases of the program. In fact, the CAARS research and development phase was concurrently underway with the acquisition phase. It seems, therefore, that at least some of DNDO's assumptions were developed in a vacuum – i.e., void of CBP input. Only when it became apparent that the CBP could not use the CAARS technology as designed did DNDO make the course correction mentioned earlier. Moreover, DNDO's Fiscal Year 2009 and Fiscal Year 2010

budget justifications failed, the GAO also reported, to reflect the full magnitude of the course correction.

In light of the fact that DNDO has not delivered a viable rad/nuc advanced radiographic solution to CBP, the lead protector of U.S. POEs, the latter agency has taken several steps to create its own solution. There is another complication, though: DHS plans to move the responsibility

for research and development of advanced radiographic imaging from DNDO to the department's Science and Technology directorate in Fiscal Year 2011. To some observers, the transition period is likely to create even greater uncertainty and fragmentation of responsibilities between CBP, DHS S&T, and DNDO. Therefore, unless DHS itself takes definitive and effective steps to ensure a greater clarity of responsibilities between and among the several agencies most directly involved, the mistakes and delays evident in the CAARS program may well be repeated.

Like many other homeland security technologies, rad/nuc detection systems must meet user application requirements. Moreover, it must be clear to all of the agencies involved that technology is an important but only one part of a comprehensive system of systems in

the protection field. Research and development of rad/nuc detection solutions therefore must be fully tested and rapidly – but safely – matured in the user's mission environment before greater investments are made in expensively broad acquisition programs. At the very heart of effective homeland security solutions is the universal need for a communicative and collaborative culture between and among the several agencies participating in this important, expensive, and technologically challenging program.

For over 10 years, the primary radiological detection systems deployed in U.S. Ports of Entry (POEs) have been Radiation Portal Monitors (RPMs), installed in both fixed and portable configurations – according to DHS, CBP now deploys an estimated 1,400 RPMs at over 300 POEs

Joseph Trindal is a career federal law enforcement investigator and executive, recently retired as chief of the Inspections & Enforcement Branch of DHS's Infrastructure Security Compliance Division. That branch is responsible for administering and enforcing the Chemical Facility Anti-Terrorism Standards.

NIMS-ICS & the Private Sector – Good Fit, or a Stretch?

By Steve Grainer, Fire/HazMat



Since the promulgation of the National Incident Management System (NIMS) almost a decade ago there has been considerable discussion of two of the primary guidelines involved. First, NIMS is intended to provide a template for consistent preparedness, prevention, mitigation, response, and recovery efforts expected to be carried out – principally by *government* entities. Second, it also is intended to create and develop a cohesive management system – i.e., the Incident Command System (ICS) – that would bring together agencies at all levels of government (local, federal, state, and tribal) to facilitate integrated command and management, one of the five basic structural components of NIMS. Fundamental to both of these assumptions is the notion that NIMS (and, therefore, ICS) is primarily, if not exclusively, designed for government use.

However, following the intense scrutiny of both NIMS and the National Response Plan in the aftermath of the 2005 hurricane season – particularly in the wake of Hurricanes Katrina and Rita – officials at all levels of government began a sometimes painful “lessons learned” process that has led to the realization that government is not – and cannot be – the only “emergency responder” called on when major events occur, particularly those of a catastrophic nature.

In fact, an interesting discovery made in the aftermath of the two hurricanes was that some of the most significant response “success stories” were achieved by the private sector. Major corporations such as Wal-Mart, Lowe’s, and Home Depot became pivotal players in the initial response operations – providing the materials, services, and support personnel desperately needed not only to meet the immediate requirements of the states and local jurisdictions involved but also to sustain long-term recovery operations.

In addition, numerous private-sector companies deployed their assets – skilled workers, equipment, and a broad spectrum of other supplies and materials – to support the federal, local, and state government responses. For example, power companies – both private corporations and “cooperatives” – deployed thousands of workers to assist in the restoration of electricity to the stricken areas. Similar support was provided by many other private utility services to restore communications and to both repair and shore up critical infrastructure – much of which, of course, was not and is not government-owned and/or operated. What is often still

overlooked, more than five years later, is the fact that those and other response efforts were neither spontaneous nor incidental.

Mutual Aid – As and When Needed

One of the key components of the NIMS Command and Management guidelines involves the quick and effective use of mutual-aid agreements, according to Steve Chafin, manager of the Emergency Preparedness Center for Dominion Virginia Power; Dominion is part of the Southeastern Electric Exchange – which is composed of 20 electric utilities that have agreed to cooperatively share their collective resources to assist other members if and when needed and requested.

The system employed by the Southeastern Electric Exchange meets what might be called the “NIMS taste test” for mutual-aid agreements. If a member utility has a need and makes a specific request for assistance, another member (or members) that can assist *will* provide the resources needed – including skilled workers. Here it is worth noting that the cooperation and coordination principles involved are usually transparent not only to the government agencies participating but also to the general public. In major cities and small towns all over the country, in fact, local residents have seen workers and supervisors from other states setting new power lines following an ice storm, flood, or other natural disaster. (Actually, the use of mutual-aid agreements started well before the 9/11 attacks and therefore pre-dates NIMS.)

At Dominion Virginia Power, according to Chafin, the company follows an “Almost NIMS” concept of emergency operations for service restoration. The term “Almost NIMS” indicates the realization that some of the terminology used by Virginia Power for many years does not directly “comply” with the NIMS guidelines. For example, if the utility receives a request for a substantial number of workers, including many specialists, to assist another member of the Exchange, the company will deploy its so-called “Dominion Contingent,” a team that typically consists of 50 to 52 personnel, including supervisors and safety specialists, as well as the equipment needed to carry out the operations for which the contingent had been requested.

Differences in Terminology Are Not Necessarily Terminal

Depending on the level of need specified, the Dominion Contingent may respond: (a) with the expectation of being accom-

modated by the requesting utility; or (b) with the capability to be fully self-sustaining – for the duration of the deployment, if necessary. For planning as well as operational purposes, however, the Contingent should be considered basically as what it is – namely, a pre-designated, pre-planned organizational structure. In NIMS terminology, therefore, the Dominion Contingent may function as a Task Force, a Strike Team, or even a geographically oriented Branch. It is not, though, an ad hoc or ad-libbed unit or organization, and in that respect is also consistent with the NIMS guidelines.

Nonetheless, and no matter what terminology is used, the Contingent’s organizational framework and tactical management are virtually the same as those described in ICS under NIMS – despite the fact that Dominion Virginia Power itself does not use those terms.

According to Steve Wood, a nuclear emergency preparedness specialist for Dominion Virginia Power, NIMS guidelines have been “adopted” for the company’s nuclear-power generation system. Dominion operates two nuclear power stations in the Commonwealth: the Surry Nuclear Power Station in southeastern Virginia; and the North Anna Nuclear Power Station in central Virginia. If and when an emergency situation starts to evolve, the company, following guidelines consistent with NIMS precepts, dispatches the personnel needed: (1) to integrate with emergency-management personnel in the Virginia Emergency Operations Center; and (2) to serve in local emergency operations centers and the Commonwealth’s Joint Information Center.

In addition, depending on the nature of the incident, the company also will provide qualified personnel to work in an “Intelligence and Investigations” capacity with local, state, and/or federal law-enforcement authorities. According to Wood, personnel in key positions are sometimes on duty assignments 24 hours a day, seven days a week. The company also has worked to achieve functional communications interoperability by developing a cache of pre-positioned equipment accessible to the key personnel responsible for carrying out pre-assigned duties.

Following the intense scrutiny of both NIMS and the National Response Plan in the wake of Hurricanes Katrina and Rita, officials at all levels of government began a sometimes painful “lessons learned” process that has led to the realization that government cannot be the only “emergency responder” called on when major events occur, particularly those of a catastrophic nature

Cooperation, Coordination & Basic Principles

Dominion Virginia Power is a member of the Institute of Nuclear Power Operations (INPO), which is based in Atlanta, Georgia. INPO routinely coordinates with all members to provide technical or specialty resources if and when needed. If an INPO member utility needs qualified radiological analysts, for example, the Institute will coordinate the search for and deployment of such specialists from other utility members. (This search-and-deploy task is yet another example of the pre-planned mutual-aid coordination consistent with, but pre-dating, the basic NIMS tenets.)

Chafin points out that Dominion Virginia Power follows a fundamental operational principle that has been successful for many years: “Centralized Planning with localized execution.” And Wood emphasizes a corollary principle – namely, that emergency management is based on *sound* management. Fundamentally, he says, “the basics are still the basics.”

Viewed in a broader context, it is obvious that the basic principles of *management*, whether for emergencies or routine operational situations, revolve around the same functional needs – Command, Planning, Operations, Logistics, and Finance and Administration, all of which are fundamental elements of the federal Incident Command System.

In short, there should and can no longer be any doubt that the private sector *must* be closely integrated with government agencies to ensure the effectiveness of comprehensive emergency-management operations. Also, if one example can serve as an appropriate leading indicator, the foundation for effective NIMS and ICS applications already exists – in the Commonwealth of Virginia. Moreover, any differences in terminology that might still exist do not necessarily, therefore, translate into any real differences in operations.

Steven Grainer is the chief of IMS programs for the Virginia Department of Fire Programs. He has served Virginia fire and emergency services and emergency management coordination since 1972 in assignments ranging from firefighter to chief officer. As a curriculum developer, content evaluator, and instructor, he currently is developing and managing VDFP programs to enable emergency responders and others to achieve NIMS compliance requirements for incident management.

WE REDUCED THE SIZE. NOT THE PROTECTION.

NIOSH
National Institute for
Occupational Safety and Health
CBRN



NHI5
ESCAPE HOOD



AVON
PROTECTION

1 888 AVON 440
www.avon-protection.com

DomPrep Survey

DHS PS-Prep Program...Raising Awareness

Prepared by Albert V. Romano, Senior Vice President, Homeland Security, Michael Baker Jr. Inc.

Supported by Dennis Schrader, President, DRS International, DP40



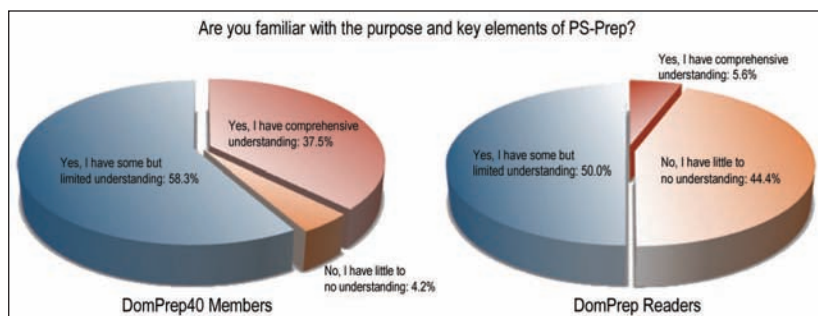
Public Law 110-53 includes a provision (Title IX, PS-Prep) for the development of a voluntary disaster preparedness certification process for private sector entities. This voluntary certification and accreditation program is being developed and managed by the Department of Homeland Security (DHS). One of the key elements of the program is the enhancement of the private sector's preparedness, readiness, and resilience to natural and manmade disasters. DHS has been leading efforts toward implementation of PS-Prep, including the development and administration of an accreditation and certification program, as well as other related standards.

To find out how familiar the preparedness, response, and recovery communities are with the PS-Prep certification process, DomPrep recently conducted a qualitative survey. The survey was conducted in September 2010, after which the responses of the DomPrep Journal readers were compared to those of the DP40 members. The majority of DP40 members and DomPrep Journal readers who responded to the survey hold upper or middle management positions within their organizations. Although many readers clicked to view the survey page, very few actually responded to the survey. This could be an indication that some readers were only peripherally interested or aware of the PS-Prep Program. The results also suggest that these readers do not yet have the understanding necessary to successfully implement the PS-Prep Program.

Key Findings: Most DomPrep Journal readers who responded are not as well versed about PS-Prep as they would like to be. Most DP40 members and readers who responded do support one or more elements of the program, though many indicated that certain elements need to be reviewed and perhaps modified.

Survey Results

First, it was important to gain an understanding of members' and readers' awareness level of PS-Prep. While 96 percent of DP40 members had at least some understanding of the program, less than 56 percent of readers could say the same.



However, roughly 90 percent of both groups would like to know more about the program. These findings, though limited, perhaps indicate that more outreach and communication is needed for a wider cross-section of DHS's stakeholders in both the public and private sectors.

The DomPrep40

The DomPrep40 is an interactive advisory board of insider practitioners and opinion leaders who have been asked to offer advice and recommendations on pertinent issues of the day. Focusing primarily on all-hazard preparedness as well as response and recovery operations, they will be challenged to provide quantifiable feedback that will be shared with the DomPrep audience.

DomPrep40 Members

John Morton

Strategic Advisor

James Augustine

Chair, EMS & Emergency Department
Physician

William Austin

Chief, West Hartford Fire Department
(West Hartford, CT)

Ann Beauchesne

Vice President, National Security &
Emergency Preparedness Department,
U.S. Chamber of Commerce

Joseph Becker

Senior Vice President, Disaster Services,
American Red Cross

Robert Blitzer

Former Chief Domestic Terrorism/Coun-
terterrorism Planning Section, National
Security Division, FBI

Bruce Clements

Public Health Preparedness Director,
Texas Department of State Health Services

John Contestabile

Former Director, Engineering &
Emergency Services, Maryland
Department of Transportation

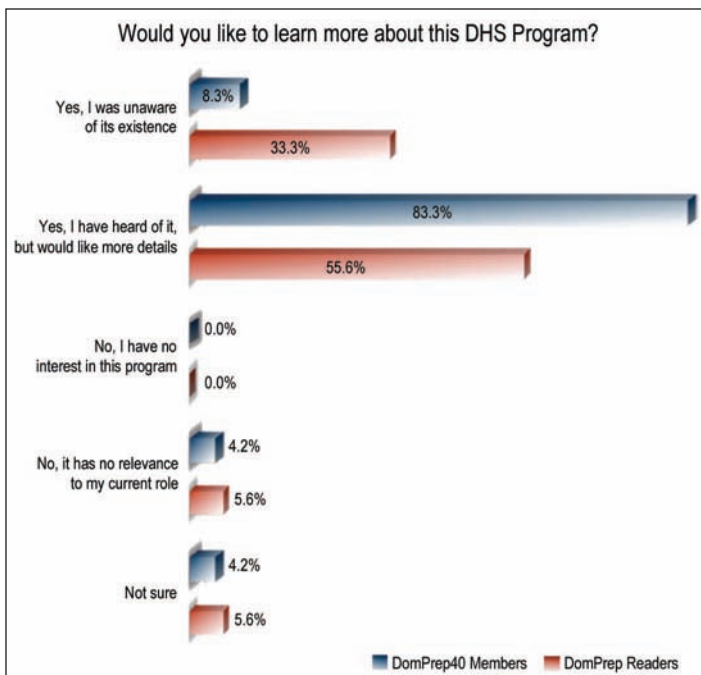
Craig DeAtley

Director for Institute for Public Health
Emergency Readiness

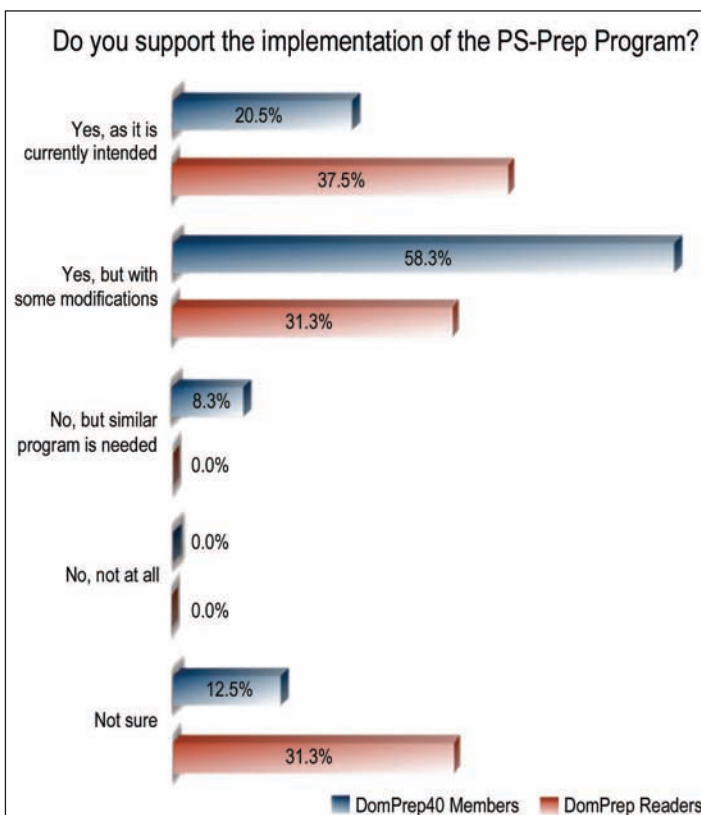
Nancy Dragani

Former President, National Emergency
Management Agency (NEMA),
Executive Director, Ohio Emergency
Management

When asked about their level of support for the PS-Prep Program, 80 percent of DP40 members, compared to 68 percent of readers, support the program as is or with some modifications. While no respondents lack support of the program in its entirety, more than a third of readers were unsure if they should support it.



The table below represents the responses of the DP40 members and the DomPrep readers to two questions about specific elements that they either support or do not support. At least some respondents supported the implementation of each element of the PS-Prep Program that was listed. Of both groups of respondents, the elements that have the greatest support are the voluntary nature as well as the accreditation and certification program. Of the elements that raised the greatest concerns, about a quarter of each group does not support the monitoring of the program. This may suggest that there is insufficient awareness as to how the program will be monitored and what the potential “compliance” requirements and remedies will be once PS-Prep is fully operational.



DomPrep40 Members

Warren Edwards

Major General USA (Ret.), Director, Community & Regional Resilience Institute (CARRI)

Katherine Fuchs

Deputy Chief FDNY Emergency Medical Services Command

Ellen Gordon

Member, Homeland Security Advisory Council and Naval Postgraduate School Center for Homeland Defense Security

Key Goss

Former Associate Director, National Preparedness Training & Exercises, FEMA

Steven Grainer

Chief, IMS Programs, Virginia Department of Fire Programs

Jack Herrmann

Senior Advisor, Public Health Preparedness, NACCHO

Cathlene Hockert

Continuity of Government Planning Director, State of Minnesota

James Hull

Vice Admiral USCG (Ret.), former Commander, Atlantic Area

Harvey Johnson, Jr.

Vice Admiral USCG (Ret.), former Deputy Administrator & Chief Operating Officer, FEMA

Dennis Jones, RN, BSN

Executive Consultant, Collaborative Fusion Inc.

Robert Kadlec

Former Special Assistant to the President for Homeland Security and Senior Director for Biological Defense Policy

Neil Livingstone

Chairman & CEO, Executive Action

James Loy

Admiral USCG (Ret.), former Deputy Secretary, DHS

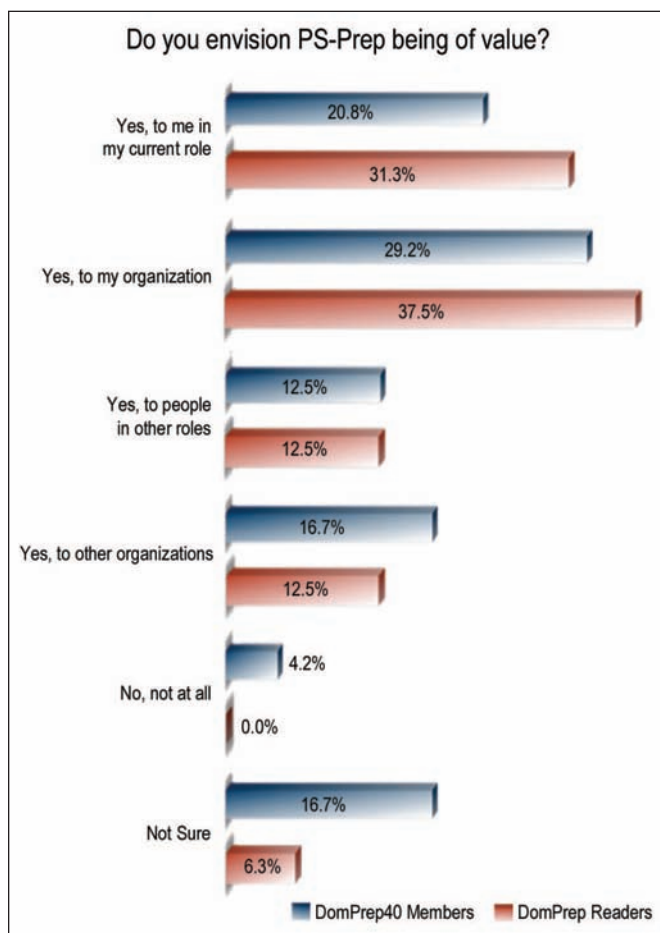
Adam McLaughlin

Preparedness Manager, Port Authority of NY & NJ (PATH)

What elements of the PS-Prep Program & its implementation do you	Support		Do Not Support	
	DomPrep40 Members	DomPrep Readers	DomPrep40 Members	DomPrep Readers
That it is voluntary	75.0%	75.0%	27.3%	21.4%
The three preparedness standards chosen	50.0%	50.0%	13.6%	14.3%
The small business considerations	54.2%	43.8%	13.6%	0.0%
The certification process	41.7%	56.3%	27.3%	21.4%
The monitoring of the program	54.2%	31.3%	27.3%	21.4%
The accreditation and certification program	58.3%	75.0%	31.8%	14.3%
None of the above	0.0%	6.3%	27.3%	57.1%

Almost 70 percent of readers who responded indicated that they envision the program as being valuable either to themselves or to others within their organizations, whereas only 50 percent of DP40 members responded similarly. However, both groups similarly believe that the program has value to others outside of their organizations. This finding suggests that, even with the limited knowledge about the program itself, there is some consensus and support regarding the intent and potential value of such a program.

The table below represents the responses to a series of questions. When asked whether there are elements of the program that should be eliminated, roughly 60 percent of



DomPrep40 Members

Vayl Oxford

Former Director, Department of Homeland Security's Domestic Nuclear Detection Office (DNDO)

Joseph Pennington

Senior Police Officer, Houston Police Department

Joseph Picciano

Deputy Director for Preparedness, NJ Office of Homeland Security & Preparedness

Stephen Reeves

Major General USA (Ret.), former Joint Program Executive Officer for Chemical & Biological Defense, DOD

Albert Romano

Senior Vice President, Homeland Security, Michael Baker Jr. Inc.

Jeff Runge

Former Chief Medical Officer, Department of Homeland Security

Richard Schoeberl

Former Executive, Federal Bureau of Investigation & the National Counterterrorism Center

Dennis Schrader

Former Deputy Administrator, National Preparedness Directorate (NPD), FEMA

Robert Stephan

Former Assistant Secretary of Homeland Security for Infrastructure Protection

Joseph Trindal

Former Director, National Capital Region, Federal Protective Service, Immigration & Customs Enforcement (ICE)

Theodore Tully

Director, Trauma & Emergency Services, Westchester Medical Center (Westchester County NY)

Craig Vanderwaghen

Former Assistant Secretary for Preparedness & Response, U.S. Department of Health & Human Services

both groups indicated that they were “not sure” at this time. This may again be indicative of the limited knowledge that many of the respondents reported about this program. Furthermore, when asked about whether the perceived benefits of the program for an organization would extend to their stakeholders – e.g., clients, insurance carriers – close to 60 percent of all respondents in both groups indicated that they would.

An interesting observation emerges when looking at the responses to the question regarding whether NOT having PS-Prep Certification or Accreditation could be a strategic disadvantage to an organization. About 31 percent of readers and 48 percent of DP40 members were not sure. These findings may suggest that there are some uncertainties about the competitive drivers or incentives required to successfully implement a voluntary program, especially given the current lack of understanding of the potential costs an organization may incur while implementing the program.

	Yes		No		Not Sure	
	DomPrep40 Members	DomPrep Readers	DomPrep40 Members	DomPrep Readers	DomPrep40 Members	DomPrep Readers
Are there elements of the PS-Prep Program that you wish to see eliminated, changed, or added?	20.8%	17.6%	12.5%	23.5%	66.7%	58.8%
Do you believe that an organization could realize benefits from its clients, customers, partners, insurance carriers, or similar stakeholders if it is designated as being “PS-Prep certified”?	56.5%	62.5%	8.7%	6.3%	34.8%	31.3%
Do you believe that not being PS-Prep certified could give an organization a competitive disadvantage?	20.8%	43.8%	29.2%	25.0%	50.0%	31.3%

One respondent stated, “I think that in the future, non-certification could have an impact on bidding procedures, etc., for companies doing business with federal and state government.” Another respondent added that “[t]here are many positive incentives that can be promoted within the voluntary framework – carrot instead of stick. Recognition, moral appeal, positive peer pressure, and negative peer pressure (i.e., black lists) [may be] needed in later phases of implementation where life safety issues are involved. This approach has worked well in voluntary seismic mitigation approaches.”

Observations from this latest survey indicate that the majority of the respondents lack a comprehensive understanding of the PS-Prep Program, but most want to learn more. They are divided about the advantages and disadvantages of certification for participating organizations as well as how the program or certification will affect them or their organizations. Among the concerns raised by respondents were questions related to incentives for compliance, the risks posed by non-compliance, and the cost to businesses. Finally, there are also some remaining questions about how such a voluntary program will be leveraged to maximize its intent and value.

Based on the results and observations of this survey, a key recommendation is that increased public awareness and understanding is needed. DHS and other stakeholders should consider expanding and accelerating outreach efforts and guidance regarding PS-Prep. A major component of this outreach effort should clearly articulate the long-term benefits PS-Prep can provide to public and private sector organizations and the nation as a whole.

For more information about the PS-Prep Program, visit the DHS website at <http://www.fema.gov/privatesector/preparedness/>.

Do You Know Someone Who Should Be Reading DomPrep.com?

Refer colleagues & coworkers to sign up today - **FREE** registration!
<http://www.DomesticPreparedness.com>



Registration Includes:

- Free access to restricted channels
- Robust archive of articles
- Huge calendar of events
- Interactivity - NEW comment section
- Access to online webinars
- Newsletter emailed every Wednesday
- PDF emailed at end of the month

The #1 Online Resource for the Preparedness & Response Community





THE MOST RELIED UPON RADIATION
DETECTOR AVAILABLE JUST GOT BETTER.

INTRODUCING identiFINDER® 2

Introducing the next generation of its world-leading radiation detector, the identiFINDER® 2. With over 10,000 identiFINDERS deployed worldwide, ICx has updated the world-leading handheld radio-isotope identification device (RIID) to provide improved nuclide identification transfective color display for ease of viewing in bright sunlight, Bluetooth®, reachback and GPS capabilities as well as a web interface.

See it for yourself at the IEEE 2010

Nuclear Science Symposium

November 2-4, 2010

Knoxville, TN

Booth # 100,102

www.icxt.com

NEW THREATS.
NEW THINKING.®



icx®
technologies

Resilience: Developing Professionalism, Clarifying the Incentives

By Dennis R. Schrader, CIP-R



The U.S. Department of Homeland Security's Quadrennial Homeland Security Review (QHSR) of February 2010 and the more recent DHS Bottoms-Up Review (BUR) of July 2010 have led to greater awareness of the importance of resilience

as a fundamental element of the nation's disaster readiness requirements. The key to improving resilience capabilities, it could be argued, will be establishing more and stronger links between government public-safety agencies and the private-sector professional continuity and engineering communities.

The QHSR focused special emphasis on the need to strengthen and mature the nation's Homeland Security Enterprise to support five principal mission areas, including resilience. The most important factor for success in achieving that goal will be the ongoing development of national security professionals who understand the entire national enterprise – i.e., federal, state, local, non-governmental, and private-sector environments and resources.

Within the next decade, it now seems probable, U.S. national-security professionals will be much more comfortable with the lexicon of resilience and therefore more capable of focusing on the tangible implementation of a more effective resilience strategy. It is currently not clear from the BUR what specifically will or should be done differently from the methods and practices of the past decade. It may simply be, of course, that focusing on resilience as a strategy could create different implementation approaches. However, it is becoming increasingly clear that there are three primary components of resilience: (a) *Community Preparedness* – not only the general population's understanding of the principal threats but also the commitment of the American people to be much better prepared; (b) *Operational Resilience* – i.e., the ability to continue operations both during and after an incident; and (c) *Systems Design* – as demonstrated by a continuing effort to build resilience into the critical infrastructure and networks during the development stage.

The most important factor for success will be the ongoing development of national security professionals who understand the entire national enterprise – i.e., federal, state, local, non-governmental, and private-sector environments and resources

Although there have been some minor successes with its resilience attempts during the past decade, the federal government has limited ability to create effective and enduring change for each of these elements through centralized Washington programs. Each of the “components” mentioned above requires an understanding of the basic incentives associated with them in order to develop workable and effective policies and programs to encourage resilience.

Core Concerns, Advance Planning, Standards, and Networks

One of the core concerns for most state and local governments, as well as private-sector businesses, is that security and disaster preparedness (SDP) will have to be included in budget planning as another “cost of doing business.” Because SDP therefore becomes a cost center, rather than a revenue center, achieving low-cost, sustainable solutions to SDP is the primary goal that will have to be pursued. One effective way to meet that goal would be by using low-cost, lightweight networks that are necessarily linked through national policy, but not directly controlled by the federal government.

For example, the most important keys to operational resilience are advance planning and business continuity. DHS recently adopted the National Fire Protection Association (NFPA) 1600 as one of its voluntary Private Sector Preparedness Standards (PS-Prep); that action could and should encourage greater resilience in the private sector.

The Disaster Recovery Institute International is an organization that has credentialed over 8,000 continuity professionals throughout the world. DRI International is, of course, now cross-referenced in NFPA 1600 as a source.

The private sector will ultimately be motivated to keep businesses operational simply to maintain profitability – which, of course, is the “prime mover” in the world's industrialized

nations. By linking with organizations such as DRI International, governments can use the business-continuity network to link the private sector to national resilience policies – and that in itself would be a considerably different way of thinking about such issues than was the custom in the past.

Another key business-continuity strategy is to focus greater attention on supply-chain networks. Because of

the Year 2000 “end of the millennium” problems, many businesses began looking more seriously at their supply-chain vulnerabilities. That effort has evolved into a routine business protocol for many if not yet all of the nation’s larger private-sector companies.

Probably the most relevant question a public safety or national security professional must now ask is, “How much do I know about organizations such as

DRI International?” The same question is valid for businesses and organizations involved in community preparedness and system design. Businesses are concerned about community preparedness in order to keep their own workforces intact. The engineering and construction community that supports the existing environment, for example, obviously wants to ensure that businesses are able to continue in operation both during and after a major incident.

SDP resources are already limited, though, and probably will be even more constrained in the future. For that reason alone, it is obvious that the more the U.S. public safety community learns to leverage private networks, the more resilient the nation will become.

Captain Dennis R. Schrader, USNR (Ret.), is president of DRS International, LLC, and former deputy administrator of the Federal Emergency Management Administration’s National Preparedness Directorate. Prior to assuming his NPD post he served as the State of Maryland’s first director of homeland security, and before that served for 16 years in various leadership posts at the University of Maryland Medical System Corporation. A licensed professional engineer in the State of Minnesota, he holds a bachelor of arts degree, with a focus in engineering, from Kettering University, and a master’s degree from the State University of New York at Buffalo. While on active duty as a Navy Civil Engineer Corps officer he served overseas tours in Guam, Diego Garcia, and Sicily. He also has served on numerous homeland-security committees, including the Anti-Terrorism Advisory Council of Maryland and the Homeland Security Senior Policy Group.



Southeast Counter-Terrorism and Emergency Response Conference and Expo

**The Blake Hotel • Charlotte, NC
November 16-18, 2010**

Conference topics include:

- **Agro-Terrorism**
- **Cyber-Terrorism**
- **Demonstration of groundbreaking COBRA system**

FREE Workshops for law enforcement, emergency management, fire & rescue and more following conference.

919-573-6108

www.SoutheastCounterTerrorismConference.com

How Clean Is Clean?

Pre-Disaster Recovery Planning: A New Focus on Deficiencies

By Jordan Nelms, Viewpoint



Earlier this month – more specifically, on 11 September – the United States observed the ninth anniversary of the most devastating terrorist attack in the nation’s history; the occasion was marked by considerable political and media commentary and academic discussions on the ability – but in some major areas of preparedness the inability – of the U.S. government to protect its citizens from the still continuing threat posed by radical Islamic terrorism. One week later, on 18 September, another key homeland security “turning point” passed with little or no discussion – namely, the ninth anniversary of the anthrax attacks on media outlets in New York City and the Washington, D.C., offices of two U.S. Democratic Senators.

An often overlooked but nonetheless major event in the chaotic establishment of the still somewhat cumbersome homeland-security mechanism that has already changed many lives and careers, the 2001 anthrax attacks must be revisited again and again until several important questions are answered. Possibly the most important of those questions is: “How clean is clean?”

After a combined effort – by the Centers for Disease Control (CDC), the Environmental Protection Agency (EPA), the Federal Bureau of Investigation (FBI), and several other federal agencies – the U.S. Postal Service (USPS) facilities in New Jersey and Washington, D.C., as well as the Hart Senate Office Building were closed, decontaminated, and eventually reopened for public use. The reoccupation of the contaminated facilities was not, though, an everyday business-as-usual process. Private-sector as well as government scientists and senior federal officials have started to realize that safety and cleanliness do not seem to be enough in themselves to change public perceptions. The debate over “How clean is clean?” is therefore one that must first be analyzed in a pre-event context so that local and national policies can focus greater attention on various ways to mitigate and reduce public reluctance to reoccupy decontaminated areas.

Earlier this year, the Department of Homeland Security (DHS) released its first draft of the National Disaster Recovery Framework (NDRF). This planning guidance document is DHS’s answer – at least part of it – to state and local agencies’ continuing need for a better coordinated approach to one of the

most important aspects of the emergency management process. In the development and promulgation of the draft NDRF, DHS left interpretation and implementation of long-term recovery policies at the state and local level somewhat open-ended. Emergency managers and many other state and local officials still have numerous questions they need answered as they begin to integrate the NDRF into their own emergency planning. It seems likely that most if not all of those answers may eventually come from several Homeland Security Inter-Agency Working Groups (IAWGs).

Although many communities throughout the nation will be focusing primarily on long-term recovery planning (from natural disasters, for the most part), the high-risk urban areas encompassed by DHS’s Urban Area Security Initiative (UASI) will also be considering and developing the recovery processes used in the wake of various “manmade” incidents and events – which are usually but not always linked to chemical, biological, radiological, and/or nuclear (CBRN) threats. The National Academies of Sciences noted in a 2003 report – *Reopening Public Facilities Following a Biological Attack* – that “decision making on the safe reoccupation of a building will be a simpler process if adequate contingency planning takes place *before* an attack [emphasis added].” Thus, the necessity of coming to a concrete determination of “How clean is clean?” becomes an important aspect of NDRF implementation.

There are three critical elements at the core of any policy developed around and involving CBRN threats and actual incidents: (1) the physical science related to CBRN threat remediation; (2) the resulting legislation developed from and involving the physical-science findings; and (3) public perceptions of, and trust in, both the science findings and the legislation enacted. With each element building on one another, the DHS IAWGs must take the initiative in standardizing the federal government’s CBRN remediation criteria. With participation by representatives of the Department of Defense (DOD), DHS, EPA, and CDC – as well as state and local emergency-management officials from the Washington, D.C., and Seattle, Washington, UASI offices – leaders of the Interagency Biological Restoration Demonstration (IBRD) conducted several “Simulation Experiments” (SIMEXs) in July 2010 to develop a comprehensive software tool that homeland-security

officials can use to develop more effective plans for the remediation operations and activities that will be required in the recovery operations mandated following any attack involving a persistent biological agent.

The IBRD is a program under the DHS Science and Technology (DHS S&T) directorate, which is charged with generating homeland security capabilities for the return of chemical/biological-contaminated areas to normal condition by funding the development of remedial strategies and technologies. In addition to developing the software tool mentioned above, the July 2010 SIMEXs – which started 14 days after a hypothetical anthrax attack – tested the interim DHS Consequence Management guidelines, which build on the official 2009 DHS *Planning Guidance for Recovery Following Biological Incidents*. S&T officials hope that the lessons learned from the SIMEXs will have a significant impact on the long-term planning for recovery and remediation operations and therefore provide at least part of the answer to the still all-important question of “How clean is clean?”

In large part because of the complexities involved in emergency management planning, only slight progress has been made to

date – more than nine years after the 2001 anthrax attacks – in developing and promulgating the policies needed to reassure the American people that CBRN-remediated facilities are in fact safe to reoccupy. As with any other planning initiative, though, “exercising” the NDRF and complementary CBRN recovery guidelines will be critical to ensure that DHS is developing and promoting planning practices that are both effective and achievable.

The development of draft guidance for general disaster recovery – and, more specifically, for the recovery from biological-specific incidents – seems to be clear evidence that DHS officials do understand the threat.

Jordan Nelms is the Homeland Security specialist at James Lee Witt Associates, where he has been responsible for homeland security consulting to state, county, municipal, and multi-jurisdictional clients around the country. Prior to joining Witt Associates, he worked in the Emergency Operations Center and Emergency Public Information Office of Pinellas County, Florida. He is also a published researcher with Johns Hopkins University's Department of Homeland Security Center of Excellence: National Center for Preparedness and Catastrophic Event Response Center (PACER).

Witt Associates is a public safety and crisis management consulting firm founded by James Lee Witt, the cabinet level director of the Federal Emergency Management Agency under President Clinton.

Emergency Preparedness & Hazmat Response Conference

Co-Sponsored by Baltimore LEPC and U.S. EPA Region III

The Nation's Premier All-Hazards Conference for Government and Industry with Quality Education, Training, and Networking



November 7-10, 2010
Hyatt Regency Inner Harbor
Baltimore, Maryland

Hosted by Baltimore Region LEPCs, Maryland Emergency Management Agency,
and Maryland Department of the Environment

IN A CHEMICAL NERVE AGENT ATTACK

Have No Regrets. Be Prepared.

By delivering the 2 recommended antidotes in an auto-injector, DuoDote® (atropine and pralidoxime chloride injection) offers the speed and simplicity to help you respond to poisoning by organophosphorous nerve agents or organophosphorous insecticides.¹⁻³

To find out more about DuoDote® and for information on grant assistance, visit www.DuoDote.com or call 1-800-638-8093.



Indication

DuoDote® Auto-Injector (atropine and pralidoxime chloride injection) is indicated for the treatment of poisoning by organophosphorous nerve agents as well as organophosphorous insecticides.

DuoDote® Auto-Injector should be administered by emergency medical services personnel who have had adequate training in the recognition and treatment of nerve agent or insecticide intoxication. DuoDote® Auto-Injector is intended as an initial treatment of the symptoms of organophosphorous insecticide or nerve agent poisoning; definitive medical care should be sought immediately.

Important Safety Information

Individuals should not rely solely upon agents such as atropine and pralidoxime to provide complete protection from chemical nerve agents and insecticide poisoning. Primary protection against exposure to chemical nerve agents and insecticide poisoning is the wearing of protective garments including masks designed specifically for this use. Evacuation and decontamination procedures should be undertaken as soon as possible. Medical personnel assisting evacuated victims of nerve agent poisoning should avoid contaminating themselves by exposure to the victim's clothing.

In the presence of life-threatening poisoning by organophosphorous nerve agents or insecticides, there are no absolute contraindications to the use of DuoDote® Auto-Injector. When symptoms of poisoning are not severe, DuoDote® Auto-Injector should be used with extreme caution in people with heart disease, arrhythmias, recent myocardial infarction, severe narrow angle glaucoma, pyloric stenosis, prostatic hypertrophy, significant renal insufficiency, chronic pulmonary disease, or hypersensitivity to any component of the product. Elderly people and children may be more susceptible to the effects of atropine. DuoDote® Auto-Injector is Pregnancy Category C and should be used during pregnancy only if the potential benefit justifies the potential risk to the fetus. Safety and effectiveness in children have not been established.

Muscle tightness and sometimes pain may occur at the injection site.

The most common side effects of atropine can be attributed to its antimuscarinic action. Pralidoxime chloride can cause changes in vision, dizziness, headache, drowsiness, nausea, tachycardia, increased blood pressure, muscular weakness, dry mouth, emesis, rash, dry skin, hyperventilation, decreased renal function, excitement, manic behavior, and transient elevation of liver enzymes and creatine phosphokinase. When atropine and pralidoxime are used together, the signs of atropinization may occur earlier than might be expected when atropine is used alone.

Please see brief summary of full Prescribing Information on adjacent page.

References: 1. Agency for Toxic Substances and Disease Registry. Medical Management Guidelines (MMGs) for nerve agents: tabun (GA); sarin (GB); soman (GD); and VX. <http://www.atsdr.cdc.gov/MHMI/mmg166.html>. Updated August 22, 2008. Accessed May 20, 2010. 2. DuoDote Auto-Injector [package insert]. Columbia, MD: Meridian Medical Technologies, Inc.; 2007. 3. Rebmann T, Clements BW, Bailey JA, Evans RG. Organophosphate antidote auto-injectors vs. traditional administration: a time motion study. *J Emerg Med.* 2009;37(2):139-143.

MERIDIAN
MEDICAL TECHNOLOGIES™

DuoDote and the DuoDote Logo are registered trademarks of Meridian Medical Technologies™, Inc., a wholly owned subsidiary of King Pharmaceuticals®, Inc. Copyright © 2010 Meridian Medical Technologies™, Inc., a wholly owned subsidiary of King Pharmaceuticals®, Inc. All rights reserved. MMT7332 08/2010



DuoDote® AUTO-INJECTOR
(atropine and pralidoxime chloride injection)

READY TO RESPOND



BRIEF SUMMARY OF FULL PRESCRIBING INFORMATION

Rx Only
Atropine 2.1 mg/0.7 mL
Pralidoxime Chloride 600 mg/2 mL

Sterile solutions for intramuscular use only

FOR USE IN NERVE AGENT AND INSECTICIDE POISONING ONLY

THE DUODOTE™ AUTO-INJECTOR SHOULD BE ADMINISTERED BY EMERGENCY MEDICAL SERVICES PERSONNEL WHO HAVE HAD ADEQUATE TRAINING IN THE RECOGNITION AND TREATMENT OF NERVE AGENT OR INSECTICIDE INTOXICATION.

INDICATIONS AND USAGE

DuoDote™ Auto-Injector is indicated for the treatment of poisoning by organophosphorus nerve agents as well as organophosphorus insecticides.

DuoDote™ Auto-Injector should be administered by emergency medical services personnel who have had adequate training in the recognition and treatment of nerve agent or insecticide intoxication.

DuoDote™ Auto-Injector is intended as an initial treatment of the symptoms of organophosphorus insecticide or nerve agent poisonings; definitive medical care should be sought immediately.

DuoDote™ Auto-Injector should be administered as soon as symptoms of organophosphorus poisoning appear (eg, usually tearing, excessive oral secretions, sneezing, muscle fasciculations).

CONTRAINDICATIONS

In the presence of life-threatening poisoning by organophosphorus nerve agents or insecticides, there are no absolute contraindications to the use of DuoDote™ Auto-Injector.

WARNINGS

CAUTION! INDIVIDUALS SHOULD NOT RELY SOLELY UPON ATROPINE AND PRALIDOXIME TO PROVIDE COMPLETE PROTECTION FROM CHEMICAL NERVE AGENTS AND INSECTICIDE POISONING.

PRIMARY PROTECTION AGAINST EXPOSURE TO CHEMICAL NERVE AGENTS AND INSECTICIDE POISONING IS THE WEARING OF PROTECTIVE GARMENTS INCLUDING MASKS DESIGNED SPECIFICALLY FOR THIS USE.

EVACUATION AND DECONTAMINATION PROCEDURES SHOULD BE UNDERTAKEN AS SOON AS POSSIBLE. MEDICAL PERSONNEL ASSISTING EVACUATED VICTIMS OF NERVE AGENT POISONING SHOULD AVOID CONTAMINATING THEMSELVES BY EXPOSURE TO THE VICTIM'S CLOTHING.

When symptoms of poisoning are not severe, DuoDote™ Auto-Injector should be used with extreme caution in people with heart disease, arrhythmias, recent myocardial infarction, severe narrow angle glaucoma, pyloric stenosis, prostatic hypertrophy, significant renal insufficiency, chronic pulmonary disease, or hypersensitivity to any component of the product. Organophosphorus nerve agent poisoning often causes bradycardia but can be associated with a heart rate in the low, high, or normal range. Atropine increases heart rate and alleviates the bradycardia. In patients with a recent myocardial infarction and/or severe coronary artery disease, there is a possibility that atropine-induced tachycardia may cause ischemia, extend or initiate myocardial infarcts, and stimulate ventricular ectopy and fibrillation. In patients without cardiac disease, atropine administration is associated with the rare occurrence of ventricular ectopy or ventricular tachycardia. Conventional systemic doses may precipitate acute glaucoma in susceptible individuals, convert partial pyloric stenosis into complete pyloric obstruction, precipitate urinary retention in individuals with prostatic hypertrophy, or cause inspersion of bronchial secretions and formation of dangerous viscid plugs in individuals with chronic lung disease.

More than 1 dose of DuoDote™ Auto-Injector, to a maximum of 3 doses, may be necessary initially when symptoms are severe. **No more than 3 doses should be administered unless definitive medical care (eg, hospitalization, respiratory support) is available.**

Severe difficulty in breathing after organophosphorus poisoning requires artificial respiration in addition to the use of DuoDote™ Auto-Injector.

A potential hazardous effect of atropine is inhibition of sweating, which in a warm environment or with exercise, can lead to hyperthermia and heat injury.

The elderly and children may be more susceptible to the effects of atropine.

PRECAUTIONS

General: The desperate condition of the organophosphorus-poisoned individual will generally mask such minor signs and symptoms of atropine and pralidoxime treatment as have been noted in normal subjects.

Because pralidoxime is excreted in the urine, a decrease in renal function will result in increased blood levels of the drug.

DuoDote™ Auto-Injector temporarily increases blood pressure, a known effect of pralidoxime. In a study of 24 healthy young adults administered a single dose of atropine and pralidoxime auto-injector intramuscularly (approximately 9 mg/kg pralidoxime chloride), diastolic blood pressure increased from baseline by 11 ± 14 mmHg (mean \pm SD), and systolic

blood pressure increased by 16 ± 19 mmHg, at 15 minutes post-dose. Blood pressures remained elevated at these approximate levels through 1 hour post-dose, began to decrease at 2 hours post-dose and were near pre-dose baseline at 4 hours post-dose. Intravenous pralidoxime doses of 30-45 mg/kg can produce moderate to marked increases in diastolic and systolic blood pressure.

Laboratory Tests: If organophosphorus poisoning is known or suspected, treatment should be instituted without waiting for confirmation of the diagnosis by laboratory tests. Red blood cell and plasma cholinesterase, and urinary parathionophenol measurements (in the case of parathion exposure) may be helpful in confirming the diagnosis and following the course of the illness. However, miosis, rhinorrhea, and/or airway symptoms due to nerve agent vapor exposure may occur with normal cholinesterase levels. Also, normal red blood cell and plasma cholinesterase values vary widely by ethnic group, age, and whether the person is pregnant. A reduction in red blood cell cholinesterase concentration to below 50% of normal is strongly suggestive of organophosphorus ester poisoning.

Drug Interactions: When atropine and pralidoxime are used together, pralidoxime may potentiate the effect of atropine. When used in combination, signs of atropinization (flushing, mydriasis, tachycardia, dryness of the mouth and nose) may occur earlier than might be expected when atropine is used alone.

The following precautions should be kept in mind in the treatment of anticholinesterase poisoning, although they do not bear directly on the use of atropine and pralidoxime.

- Barbiturates are potentiated by the anticholinesterases; therefore, barbiturates should be used cautiously in the treatment of convulsions.
- Morphine, theophylline, aminophylline, succinylcholine, reserpine, and phenothiazine-type tranquilizers should be avoided in treating personnel with organophosphorus poisoning.
- Succinylcholine and mivacurium are metabolized by cholinesterases. Since pralidoxime reactivates cholinesterases, use of pralidoxime in organophosphorus poisoning may accelerate reversal of the neuromuscular blocking effects of succinylcholine and mivacurium.

Drug-drug interaction potential involving cytochrome P450 isozymes has not been studied.

Carcinogenesis, Mutagenesis, Impairment of Fertility: DuoDote™ Auto-Injector is indicated for short-term emergency use only, and no adequate studies regarding the potential of atropine or pralidoxime chloride for carcinogenesis or mutagenesis have been conducted.

Impairment of Fertility: In studies in which male rats were orally administered atropine (62.5 to 125 mg/kg) for one week prior to mating and throughout a 5-day mating period with untreated females, a dose-related decrease in fertility was observed. A no-effect dose for male reproductive toxicity was not established. The low-effect dose was 290 times (on a mg/m² basis) the dose of atropine in a single application of DuoDote™ Auto-Injector (2.1 mg).

Fertility studies of atropine in females or of pralidoxime in males or females have not been conducted.

Pregnancy:

Pregnancy Category C: Adequate animal reproduction studies have not been conducted with atropine, pralidoxime, or the combination. It is not known whether pralidoxime or atropine can cause fetal harm when administered to a pregnant woman or if they can affect reproductive capacity. Atropine readily crosses the placental barrier and enters the fetal circulation.

DuoDote™ Auto-Injector should be used during pregnancy only if the potential benefit justifies the potential risk to the fetus.

Nursing Mothers: Atropine has been reported to be excreted in human milk. It is not known whether pralidoxime is excreted in human milk. Because many drugs are excreted in human milk, caution should be exercised when DuoDote™ Auto-Injector is administered to a nursing woman.

Pediatric Use: Safety and effectiveness of DuoDote™ Auto-Injector in pediatric patients have not been established.

ADVERSE REACTIONS

Muscle tightness and sometimes pain may occur at the injection site.

Atropine

The most common side effects of atropine can be attributed to its antimuscarinic action. These include dryness of the mouth, blurred vision, dry eyes, photophobia, confusion, headache, dizziness, tachycardia, palpitations, flushing, urinary hesitancy or retention, constipation, abdominal pain, abdominal distention, nausea and vomiting, loss of libido, and impotence. Anhidrosis may produce heat intolerance and impairment of temperature regulation in a hot environment. Dysphagia, paralytic ileus, and acute angle closure glaucoma, maculopapular rash, petechial rash, and scarlatiniform rash have also been reported.

Larger or toxic doses may produce such central effects as restlessness, tremor, fatigue, locomotor difficulties, delirium followed by hallucinations, depression, and, ultimately medullary paralysis and death. Large doses can also lead to circulatory collapse. In such cases, blood pressure declines and death due to respiratory failure may ensue following paralysis and coma.

Cardiovascular adverse events reported in the literature for atropine include, but are not limited to, sinus tachycardia, palpitations, premature ventricular contractions, atrial flutter, atrial fibrillation, ventricular flutter, ventricular fibrillation, cardiac syncope, asystole, and myocardial infarction. (See **PRECAUTIONS**.)

Hypersensitivity reactions will occasionally occur, are usually seen as skin rashes, and may progress to exfoliation. Anaphylactic reaction and laryngospasm are rare.

Pralidoxime Chloride

Pralidoxime can cause blurred vision, diplopia and impaired accommodation, dizziness, headache, drowsiness, nausea, tachycardia, increased systolic and diastolic blood pressure, muscular weakness, dry mouth, emesis, rash, dry skin, hyperventilation, decreased renal function, and decreased sweating when given parenterally to normal volunteers who have not been exposed to anticholinesterase poisons.

In several cases of organophosphorus poisoning, excitement and manic behavior have occurred immediately following recovery of consciousness, in either the presence or absence of pralidoxime administration. However, similar behavior has not been reported in subjects given pralidoxime in the absence of organophosphorus poisoning.

Elevations in SGOT and/or SGPT enzyme levels were observed in 1 of 6 normal volunteers given 1200 mg of pralidoxime intramuscularly, and in 4 of 6 volunteers given 1800 mg intramuscularly. Levels returned to normal in about 2 weeks. Transient elevations in creatine kinase were observed in all normal volunteers given the drug.

Atropine and Pralidoxime Chloride

When atropine and pralidoxime are used together, the signs of atropinization may occur earlier than might be expected when atropine is used alone.

OVERDOSAGE

Symptoms:

Atropine

Manifestations of atropine overdose are dose-related and include flushing, dry skin and mucous membranes, tachycardia, widely dilated pupils that are poorly responsive to light, blurred vision, and fever (which can sometimes be dangerously elevated). Locomotor difficulties, disorientation, hallucinations, delirium, confusion, agitation, coma, and central depression can occur and may last 48 hours or longer. In instances of severe atropine intoxication, respiratory depression, coma, circulatory collapse, and death may occur.

The fatal dose of atropine is unknown. In the treatment of organophosphorus poisoning, doses as high as 1000 mg have been given. The few deaths in adults reported in the literature were generally seen using typical clinical doses of atropine often in the setting of bradycardia associated with an acute myocardial infarction, or with larger doses, due to overheating in a setting of vigorous physical activity in a hot environment.

Pralidoxime

It may be difficult to differentiate some of the side effects due to pralidoxime from those due to organophosphorus poisoning. Symptoms of pralidoxime overdose may include: dizziness, blurred vision, diplopia, headache, impaired accommodation, nausea, and slight tachycardia. Transient hypertension due to pralidoxime may last several hours.

Treatment: For atropine overdose, supportive treatment should be administered. If respiration is depressed, artificial respiration with oxygen is necessary. Ice bags, a hypothermia blanket, or other methods of cooling may be required to reduce atropine-induced fever, especially in children. Catheterization may be necessary if urinary retention occurs. Since atropine elimination takes place through the kidney, urinary output must be maintained and increased if possible; intravenous fluids may be indicated. Because of atropine-induced photophobia, the room should be darkened.

A short-acting barbiturate or diazepam may be needed to control marked excitement and convulsions. However, large doses for sedation should be avoided because central depressant action may coincide with the depression occurring late in severe atropine poisoning. Central stimulants are not recommended.

Physostigmine, given as an atropine antidote by slow intravenous injection of 1 to 4 mg (0.5 to 1.0 mg in children) rapidly abolishes delirium and coma caused by large doses of atropine. Since physostigmine has a short duration of action, the patient may again lapse into coma after 1 or 2 hours, and require repeated doses. Neostigmine, pilocarpine, and methacholine are of little benefit, since they do not penetrate the blood-brain barrier.

Pralidoxime-induced hypertension has been treated by administering phentolamine 5 mg intravenously, repeated if necessary due to phentolamine's short duration of action. In the absence of substantial clinical data regarding use of phentolamine to treat pralidoxime-induced hypertension, consider slow infusion to avoid precipitous corrections in blood pressure.

MERIDIAN MEDICAL TECHNOLOGIES

© 2010 Meridian Medical Technologies™, Inc., a subsidiary of King Pharmaceuticals®, Inc.
Manufactured by Meridian Medical Technologies™, Inc.
Columbia, MD 21046
DuoDote and the DuoDote Logo are registered trademarks of Meridian Medical Technologies™, Inc.
MMT 5173 02/2010

Gauging the Threat of an Electromagnetic Pulse (EMP) Attack

By Scott Stewart & Nathan Hughes, Viewpoint



The following article is reprinted with permission of Stratfor Global Intelligence. The opinions expressed herein do not necessarily represent the views of DomesticPreparedness.com, but should be shared with DomPrep readers.

Over the past decade there has been an ongoing debate over the threat posed by electromagnetic pulse (EMP) to modern civilization. This debate has been the most heated perhaps in the United States, where the commission appointed by Congress to assess the threat to the United States warned of the dangers posed by EMP in reports released in 2004 and 2008. The commission also called for a national commitment to address the EMP threat by hardening the national infrastructure.

There is little doubt that efforts by the United States to harden infrastructure against EMP – and its ability to manage critical infrastructure manually in the event of an EMP attack – have been eroded in recent decades as the Cold War ended and the threat of nuclear conflict with Russia lessened. This is also true of the U.S. military, which has spent little time contemplating such scenarios in the years since the fall of the Soviet Union. The cost of remedying the situation, especially retrofitting older systems rather than simply regulating that new systems be better hardened, is immense. And as with any issue involving massive amounts of money, the debate over guarding against EMP has become quite politicized in recent years.

We have long avoided writing on this topic for precisely that reason. However, as the debate over the EMP threat has continued, a great deal of discussion about the threat has appeared in the media. Many STRATFOR readers have asked for our take on the threat, and we thought it might be helpful to dispassionately discuss the tactical elements involved in such an attack and the various actors that could conduct one. The following is our assessment of the likelihood of an EMP attack against the United States.

Defining Electromagnetic Pulse

EMP can be generated from natural sources such as lightning or solar storms interacting with the earth's

atmosphere, ionosphere and magnetic field. It can also be artificially created using a nuclear weapon or a variety of non-nuclear devices. It has long been proven that EMP can disable electronics. Its ability to do so has been demonstrated by solar storms, lightning strikes and atmospheric nuclear explosions before the ban on such tests. The effect has also been recreated by EMP simulators designed to reproduce the electromagnetic pulse of a nuclear device and study how the phenomenon impacts various kinds of electrical and electronic devices such as power grids, telecommunications and computer systems, both civilian and military.

The effects of an EMP – both tactical and strategic – have the potential to be quite significant, but they are also quite uncertain. Such widespread effects can be created during a high-altitude nuclear detonation (generally above 30 kilometers, or about 18 miles). This widespread EMP effect is referred to as high-altitude EMP or HEMP. Test data from actual high-altitude nuclear explosions is extremely limited. Only the United States and the Soviet Union conducted atmospheric nuclear tests above 20 kilometers and, combined, they carried out fewer than 20 actual tests.

As late as 1962 – a year before the Partial Test Ban Treaty went into effect, prohibiting its signatories from conducting aboveground test detonations and ending atmospheric tests – scientists were surprised by the HEMP effect. During a July 1962 atmospheric nuclear test called “Starfish Prime,” which took place 400 kilometers above Johnston Island in the Pacific, electrical and electronic systems were damaged in Hawaii, some 1,400 kilometers away. The Starfish Prime test was not designed to study HEMP, and the effect on Hawaii, which was so far from ground zero, startled U.S. scientists.

High-altitude nuclear testing effectively ended before the parameters and effects of HEMP were well understood. The limited body of knowledge that was gained from these tests remains a highly classified matter in both the United States and Russia. Consequently, it is difficult to speak intelligently about EMP or publicly debate the precise nature of its effects in the open-source arena.

The importance of the EMP threat should not be understated. There is no doubt that the impact of a HEMP attack would be significant. But any actor plotting such an attack would be dealing with immense uncertainties – not only about the ideal altitude at which to detonate the device based on its design and yield in order to maximize its effect but also about the nature of those effects and just how devastating they could be.

Non-nuclear devices that create an EMP-like effect, such as high-power microwave (HPM) devices, have been developed by several countries, including the United States. The most capable of these devices are thought to have significant tactical utility and more powerful variants may be able to achieve effects more than a kilometer away. But at the present time, such weapons do not appear to be able to create an EMP effect large enough to affect a city, much less an entire country. Because of this, we will confine our discussion of the EMP threat to HEMP caused by a nuclear detonation, which also happens to be the most prevalent scenario appearing in the media.

Attack Scenarios

In order to have the best chance of causing the type of immediate and certain EMP damage to the United States on a continent-wide scale, as discussed in many media reports, a nuclear weapon (probably in the megaton range) would need to be detonated well above 30 kilometers somewhere over the American Midwest. Modern commercial aircraft cruise at a third of this altitude. Only the United States, United Kingdom, France, Russia and China possess both the mature warhead design and intercontinental ballistic missile (ICBM) capability to conduct such an attack from their own territory, and these same countries have possessed that capability for decades. (Shorter range missiles can achieve this altitude, but the center of the United States is still 1,000 kilometers from the Eastern Seaboard and more than 3,000 kilometers from the Western Seaboard – so just any old Scud missile won't do.)

The HEMP threat is nothing new. It has existed since the early 1960s, when nuclear weapons were first mated with ballistic missiles, and grew to be an important component of nuclear strategy. Despite the necessarily limited understanding of its effects, both the United States and Soviet Union almost certainly included the use of weapons to create HEMPs in both defensive and especially offensive scenarios, and both post-

Soviet Russia and China are still thought to include HEMP in some attack scenarios against the United States.

However, there are significant deterrents to the use of nuclear weapons in a HEMP attack against the United States, and nuclear weapons have not been used in an attack anywhere since 1945. Despite some theorizing that a HEMP attack might be somehow less destructive and therefore less likely to provoke a devastating retaliatory response, such an attack against the United States would inherently and necessarily represent a nuclear attack on the U.S. homeland and the idea that the United States would not respond in kind is absurd. The United States continues to maintain the most credible and survivable nuclear deterrent in the world, and any actor contemplating a HEMP attack would have to assume not that they might experience some limited reprisal but that the U.S. reprisal would be full, swift and devastating.

Countries that build nuclear weapons do so at great expense. This is not a minor point. Even today, a successful nuclear weapons program is the product of years – if not a decade or more – and the focused investment of a broad spectrum of national resources. Nuclear weapons also are developed as a deterrent to attack, not with the intention of immediately using them offensively. Once a design has achieved an initial capability, the focus shifts to establishing a survivable deterrent that can withstand first a conventional and then a nuclear first strike so that the nuclear arsenal can serve its primary purpose as a deterrent to attack. The coherency, skill and focus this requires are difficult to overstate and come at immense cost – including opportunity cost – to the developing country. The idea that Washington will interpret the use of a nuclear weapon to create a HEMP as somehow less hostile than the use of a nuclear weapon to physically destroy an American city is not something a country is likely to gamble on.

In other words, for the countries capable of carrying out a HEMP attack, the principles of nuclear deterrence and the threat of a full-scale retaliatory strike continue to hold and govern, just as they did during the most tension-filled days of the Cold War.

Rogue Actors


One scenario that has been widely put forth is that the EMP threat emanates not from a global or regional power like Russia or China but from a rogue state or a transnational terrorist group that does not possess ICBMs but will use subterfuge to accomplish its mission without leaving any fingerprints. In

this scenario, the rogue state or terrorist group loads a nuclear warhead and missile launcher aboard a cargo ship or tanker and then launches the missile from just off the coast in order to get the warhead into position over the target for a HEMP strike. This scenario would involve either a short-range ballistic missile to achieve a localized metropolitan strike or a longer-range (but not intercontinental) ballistic missile to reach the necessary position over the Eastern or Western seaboard or the Midwest to achieve a key coastline or continental strike.

When we consider this scenario, we must first acknowledge that it faces the same obstacles as any other nuclear weapon employed in a terrorist attack. It is unlikely that a terrorist group like al Qaeda or Hezbollah can develop its own nuclear weapons program. It is also highly unlikely that a nation that has devoted significant effort and treasure to develop a nuclear weapon would entrust such a weapon to an outside organization. Any use of a nuclear weapon would be vigorously investigated and the nation that produced the weapon would be identified and would pay a heavy price for such an attack (there has been a large investment in the last decade in nuclear forensics). Lastly, as noted above, a nuclear weapon is seen as a deterrent by countries such as North Korea or Iran, which seek such weapons to protect themselves from invasion, not to use them offensively. While a group like al Qaeda would likely use a nuclear device if it could obtain one, we doubt that other groups such as Hezbollah would. Hezbollah has a known base of operations in Lebanon that could be hit in a counterstrike and would therefore be less willing to risk an attack that could be traced back to it.

Also, such a scenario would require not a crude nuclear device but a sophisticated nuclear warhead capable of being mated with a ballistic missile.


There are considerable technical barriers that separate a crude nuclear device from a sophisticated nuclear warhead. The engineering expertise required to construct such a warhead is far greater than that required to construct a crude device. A warhead must be far more compact than a primitive device. It must also have a trigger mechanism and electronics and physics packages capable of withstanding the force of an ICBM launch, the journey into the cold



If This Is Your Crisis Plan For Chemical & Bio Hazards? Get A Better Plan!

The AP4C Handheld Chemical Detector

- ▶ Fast Start-Up
- ▶ No Shelf Cost
- ▶ Easy to Use



Contact Us Now, Before It's Too Late...

PROENGINE

vacuum of space and the heat and force of re-entering the atmosphere – and still function as designed. Designing a functional warhead takes considerable advances in several fields of science, including physics, electronics, engineering, metallurgy and explosives technology, and overseeing it all must be a high-end quality assurance capability. Because of this, it is our estimation that it would be far simpler for a terrorist group looking to conduct a nuclear attack to do so using a crude device than it would be using a sophisticated warhead – although we assess the risk of any non-state actor obtaining a nuclear capability of any kind, crude or sophisticated, as extraordinarily unlikely.

But even if a terrorist organization were somehow able to obtain a functional warhead and compatible fissile core, the challenges of mating the warhead to a missile it was not designed for and then getting it to launch and detonate properly would be far more daunting than it would appear at first glance. Additionally, the process of fueling a liquid-fueled ballistic missile at sea and then launching it from a ship using an improvised launcher would also be very challenging. (North Korea, Iran and Pakistan all rely heavily on Scud technology, which uses volatile, corrosive and toxic fuels.)

Such a scenario is challenging enough, even before the uncertainty of achieving the desired HEMP effect is taken into account. This is just the kind of complexity and uncertainty that well-trained terrorist operatives seek to avoid in an operation. Besides, a ground-level nuclear detonation in a city such as New York or Washington would be more likely to cause the type of terror, death and physical destruction that is sought in a terrorist attack than could be achieved by generally non-lethal EMP.

Make no mistake: EMP is real. Modern civilization depends heavily on electronics and the electrical grid for a wide range of vital functions, and this is truer in the United States than in most other countries. Because of this, a HEMP attack or a substantial geomagnetic storm could have a dramatic impact on modern life in the affected area. However, as we've discussed, the EMP threat has been around for more than half a century and there are a number of technical and practical variables that make a HEMP attack using a nuclear warhead highly unlikely.

When considering the EMP threat, it is important to recognize that it exists amid a myriad other threats, including related

threats such as nuclear warfare and targeted, small-scale HPM attacks. They also include threats posed by conventional warfare and conventional weapons such as man-portable air-defense systems, terrorism, cyberwarfare attacks against critical infrastructure, chemical and biological attacks – even natural disasters such as earthquakes, hurricanes, floods and tsunamis.

The world is a dangerous place, full of potential threats. Some things are more likely to occur than others, and there is only a limited amount of funding to monitor, harden against, and try to prevent, prepare for and manage them all. When one attempts to defend against everything, the practical result is that one defends against nothing. Clear-sighted, well-grounded and rational prioritization of threats is essential to the effective defense of the homeland.

Hardening national infrastructure against EMP and HPM is undoubtedly important, and there are very real weaknesses and critical vulnerabilities in America's critical infrastructure – not to mention civil society. But each dollar spent on these efforts must be balanced against a dollar not spent on, for example, port security, which we believe is a far more likely and far more consequential vector for nuclear attack by a rogue state or non-state actor.

This report may be forwarded or republished on your website with attribution to www.stratfor.com.

Copyright 2010 STRATFOR

Scott Stewart is STRATFOR's VP, Tactical Intelligence. He is a former Diplomatic Security Service Special Agent who was involved in hundreds of terrorism investigations, most notably the 1993 World Trade Center bombing and the follow-on New York City bomb plot investigation, during which he served as lead investigator for the U.S. State Department. He led a team of Americans who aided the government of Argentina in investigating the 1992 bombing of the Israeli Embassy in Buenos Aires, and was involved in investigations following a series of attacks and attempted attacks by the Iraqi intelligence service during the first Gulf War.

Nathan Hughes is STRATFOR's Director of Military Analysis, covering strategic defense issues around the globe and providing military context for wider geopolitical analysis. He monitors ongoing military conflict and emerging trends including missile technology proliferation, ballistic missile defense and the weaponization of space. His focus areas include the war in Afghanistan, naval developments and strategic nuclear forces.

They Expect You To Be More Than 80%* Prepared for a Biological Threat



Now You Can Be with the New **RAZOR™ EX**



RAZOR EX

Field Portable BioHazard Detection System

Less than 1% error rate

Screen ten targets in a single run with The 10™ Target Kit

Used by Military, Hazmat, and First Responders

The 10™ Target Screen Kit:

Anthrax	<i>E. coli</i> O157	<i>Salmonella</i>
<i>Brucella</i> spp.	Tularemia	Smallpox
Botulism	Ricin	Plague
<i>Coxiella</i>		



Call **1.800.735.8544** or visit www.idahotech.com to discover how you can reliably protect those you serve.

*Most other field biohazard detectors have a 20% error rate.



390 Wakara Way, Salt Lake City, UT, 84108, USA | 1-800-735-6544 | www.idahotech.com

Louisiana, Alabama, New Jersey, and Washington

By Adam McLaughlin, State Homeland News



Louisiana Parishes Develop & Coordinate New Evacuation System

After the evacuees were out of the Monroe Civic Center and all the repairs possible had been made, local officials joined the rest of the state in spelling out and studying the lessons learned in 2005 from Hurricanes Katrina and Rita.

Five years later, these same local officials have partnered with various parishes on a number of matters, including ways to make south-to-north evacuations within the state as smooth and as safe as possible. Monroe's city officials have already reached agreements with three parishes, for example, on what they call a "point-to-point system" – which everyone involved hopes will bring a more effective structure to the evacuation process. More specifically, Monroe has reached "cooperative endeavor" agreements with Terrebonne, Lafourche, and St. John the Baptist parishes. Under those agreements, Terrebonne Parish evacuees have been pre-designated to go to the Monroe Civic Center, and the Harvey H. Benoit and Emily Parker Robinson Community Centers will serve as shelters for evacuees from Lafourche Parish.

Monroe Mayor Jamie Mayo said the principal lesson learned from the back-to-back hurricanes in 2005 is the importance of communication. "Communication was the most important thing during Katrina and Rita as well as Gustav and Ike," Mayo said. "That [experience] has enabled us to put together a strong response plan, which is critical in responding to devastating national disasters and general catastrophes." This is the first year for the plan – which Mayo believes is the only one of its kind in the state – to be in effect.

The partnership with parishes in the same general area of the state will allow officials to keep better track of evacuees. They also will be able to send extra staff, such as police, to provide security at local shelters within the parishes designated.

Butch Beckham, director of the Ouachita Parish Office of Homeland Security and Emergency Preparedness, said the point-to-point system has a number of particularly helpful aspects. When evacuees arrive at their pre-designated shelters, for example, they will register and be provided with armbands – which, Beckham said, will help officials quickly locate the shelter of a family member or friend when anyone asks about them.

The partnership with parishes in the same general area of the state will allow officials to keep better track of evacuees; they also will be able to send extra staff, such as police, to provide security at local shelters within the parishes designated

The agreements also stipulate that: (a) the participating parishes will be responsible for any damages to the facilities while evacuees are housed there; and (b) With a 48-hour notice to the city of Monroe before arriving, the parishes will be responsible for overtime pay for community-center workers and security staff.

Mayo has requested that more than \$1 million in funds be provided from the state Office of Homeland Security and Emergency Preparedness for renovations to the shelter recreation centers to make them more comfortable and more helpful when they are being used by evacuees. The renovations will also benefit the community at large, of course.

One of Mayo's principal concerns is ensuring that there will be an adequate number of restrooms and showers available. "I have talked to [Louisiana] Governor [Bobby] Jindal about the request for funds," Mayo said. "There are shower issues and other challenges that [still] need to be addressed."

Note: In a closely related development, the city of West Monroe recently secured similar funds for its West Ouachita Senior Center. West Monroe officials said they plan to use that money to enlarge and upgrade the bathrooms in the shelter, and to add a bus barn, a triage room, and a laundry.

NEW

CHEMPRO

Handheld Chemical Detector **100i**

ChemPro100i is a handheld vapor detector for classification of Chemical Warfare Agents (CWAs) and Toxic Industrial Chemicals (TICs). The ChemPro100i adds 6 more sensors to increase the number of chemicals that it can detect and to decrease the potential for false alarms.



No maintenance costs for 5 years!

- Industry leading sensitivity
- Stores well - no regular exercise needed
- Non-threatening design
- Easy-to-use

* Contact Us for details on our standard 5-years Guaranteed Cost of Ownership (GCO) program



Environics Oy
Graanintie 5
P.O. Box 349
FI-50101 Mikkeli, Finland
tel. +358 201 430 430
fax. +358 201 430 440
www.environics.fi
sales@environics.fi

Environics USA Inc.
1308 Continental Drive, Suite J
Abingdon, MD 21009
USA
tel. +1 (410) 612-1250
fax. +1 (410) 612-1251
www.EnvironicsUSA.com
sales@EnvironicsUSA.com

Alabama Homeland Security Drill Offers Rare Look at Disaster Preparedness

The U.S. Department of Homeland Security's Center for Domestic Preparedness (CDP) invited the media for a rare and close look, late last month, at two different health care training exercises, both of which seemed to come together as one.

In the scenario, health care workers from cities throughout the United States acted out a simulated "explosion" at a battery acid factory. Numerous "patients" showed up bleeding and/or in various states of shock and hysteria. More and more casualties continued to arrive, and workers had to set up a decontamination station outside the emergency room.

The CDP operates on the site of the old Fort McClellan Army base. Last month's exercise took place at the Noble Training Center, which once served as the base hospital. The CDP had been training first responders from all over the country on various "nightmare" terrorism scenarios even before the 9/11 terrorist attacks. The CDP training exercises teach responders about a broad spectrum of lethal incidents and dangerous "situations" of various types ranging from hurricanes to the operation of meth labs in cars, attics, or other unlikely locales.

"There is just a heightened sense of urgency" in the CDP exercises, said student Irene Thompson, who works at a hospital in Maryland. "It [the realistic training] is not like sitting in a classroom, where you are talking about it. We are actually doing it."

Lanny Campbell, a doctor from Idaho, said he saw "numerous obstacles" thrown at him during the exercise. At one point, a generator failure shut down power at the hospital, as part of the drill. "It ... [was] quite overwhelming, but it helped me prepare a little bit," said Campbell.

Trainers say that the difficult training helps responders cope with "almost everything" they are likely to encounter later

in their careers. "Essentially," health care course manager Candice Gilliland said, "what they bring back is a little bit more knowledge to go back and check their emergency-operations plan at their facility, and check and see, 'hey, do we have this accounted for, can we or are we prepared for this?'" Another course manager, John Skinner, described how world events – from terrorism to natural disasters – shape what happens at the center. "We are trying to keep up with the [real-life] incidents that are happening throughout the world," he commented. "We have had Katrina, which was

a major incident for the United States, we have had fires, we have had floods, and every single one of those [incidents] produced large numbers of casualties."

The CDP courses are funded entirely from the federal DHS (Department of Homeland Security) budget. This allows state and local hospitals, police and fire departments, and other agencies to participate in extremely valuable training exercise without having to reallocate their own funds.

In the Information Age, as decision-making officials at all levels of government seek to connect with the public more quickly – and, if possible, to everyone at the same time – the social media have become an increasingly valuable communications tool

New Jersey Emergency Alert System Links 39 Towns Via Social Media

In March, a powerful storm pummeled New Jersey, forcing police, utility, and emergency crews throughout the state to scramble as the severe weather sapped power, delayed trains, and in some areas even triggered floods. But publicly available information about the storm's effects was scarce, and citizens searching for updates were left high if not dry.

To avert such communication failures in the future, in early September, when Hurricane Earl had its sights set on New Jersey, Morris County's OEM (Office of Emergency Management) officials activated a shared emergency information network that uses social media tools – Facebook and Twitter – to deliver crucial updates around the clock.

The emergency alert system, dubbed MCUrgent, enables the county OEM to issue notifications and warnings to area residents. Ultimately, the shared network will provide a

platform for each of the county's 39 towns to quickly share and disseminate emergency information whenever disaster strikes. MCUrgent is "a shared service," said Carol Spencer, webmaster of the county's Information Technology department. "Our goal right now is multi-jurisdictional emergency management."

In the Information Age, as decision-making officials at all levels of government seek to connect with the public more quickly – and, if possible, to everyone at the same time – the social media have become an increasingly valuable communications tool. Facebook, Twitter, and other social-media sites help governments disseminate important information in a few keystrokes. Users can access the data immediately through their computers or mobile devices.

These digital "news blasts" are particularly appealing to emergency managers who want to spread the word as quickly as possible about road closings, power outages, flash floods, and various related problems and inconveniences, as well as the locations of emergency shelters. Some local agencies, such as the Philadelphia OEM, have been taking advantage of tools like Facebook, Twitter, YouTube, and LinkedIn for several years.

Because of the successes elsewhere, Morris County officials decided to take the concept to a new level by linking with local municipalities in one shared network. Margaret Nordstrom, a Morris County freeholder (an office similar to that of a county supervisor), played a key role in pushing the social-media strategy, Spencer said, "where we are capturing the information at its source and aggregating it on our websites."

In the next phase of the program, the county plans to select its platform of choice and connect with interested municipalities. The Morris County OEM already has nearly 100 fans on its new Facebook page, and 29 Twitter followers. On Twitter, citizens can contribute directly by posting messages through the use of "hashtags," set up by the county, that will identify each municipality. They can also receive messages via text.

The alerts will be restricted to emergency information only. But, as Spencer points out, the new system will not necessarily be the "end-all, be-all" solution. In fact, MCUrgent may simply represent – for the time being, at least – an additional notification tool that will spread information and warnings, and help provide coverage 24 hours a day, seven days a week.

Washington **Evergreen State Receives** **Over \$1 Million for Seismic Retrofits**

In early September, the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) allocated \$1,092,347 in HMGP (Hazard Mitigation Grant Program) funds to the state of Washington for a "seismic retrofitting" of Hall A at the Evergreen State College's Dormitory Residence, which houses 173 students during the school year, as well as the administrative offices of the college's Residential and Dining Services. During summer months, Hall A is used to host summer programs and house conference participants.

According to FEMA Regional Administrator Kenneth Murphy, the seismic retrofit project will bring the facility up to current seismic code. The 10-story Hall A, he points out, is the tallest building on campus. The planned seismic reinforcement capability will help enhance occupant safety in the event of a moderate-to-strong earthquake.

According to James Mullen, director of the Washington Emergency Management Division (WEMD), "It is very satisfying when projects of this nature get funded. We [Washington] are number two among the states in earthquake risk, and this work is one more step toward enhancing life safety for our citizens."

FEMA is contributing 75 percent of the total cost of the \$1,456,463 project; WEMD, which administers the program in Washington State, is providing the remaining 25 percent. The HMGP provides funding for cost-effective projects designed to prevent damage and minimize injuries during future times of disaster.

Adam McLaughlin currently serves as the Manager of Emergency Readiness, Office of Emergency Management, for the Port Authority of New York and New Jersey. His responsibilities include both the development and coordination of Port Authority interagency all-hazards plans and the design and development of emergency preparedness exercises. A Certified Emergency Manager (CEM), he is a former U.S. Army officer – and a veteran of the war in Afghanistan – and a member of the Faculty of Senior Fellows for the Long Island University's Homeland Security Management Institute.

SAVE THE DATE!

OCTOBER 30– NOVEMBER 4, 2010

VISIT US IN BOOTH 621

Talk the Talk—
now,
Walk
the Walk



58TH IAEM ANNUAL CONFERENCE & EMEX 2010

HILTON PALACIO DEL RIO & HENRY B. GONZALEZ CONVENTION CENTER · SAN ANTONIO, TEXAS, USA

Join us in San Antonio for this informative event!

At the 2010 IAEM Annual Conference, you'll have an opportunity to network and exchange ideas with more than 1,500 others in the emergency management and homeland security fields. Attendees will benefit from educational forums on current industry trends and tools, as well as professional training. While you're here, plan to visit EMEX 2010—the showcase for leading technologies, products and services in emergency management.



Keynote Speaker

W. Craig Fugate
*Administrator of the
Federal Emergency
Management Agency*

For more information on
how you can join us, visit
www.iaem.com.

Other Featured Speakers

Janine Driver
Body Language Expert

Margaret Davidson
Director of the NOAA Coastal Services Center

Ana-Marie Jones
*Executive Director of CARD—Collaborating
Agencies Responding to Disasters*

Madhu Beriwal
President and CEO of IEM



Who Should Attend:

Emergency Managers
Homeland Security Officials
First Response Coordinators
Contingency Planners
Private Industry Risk Managers
Operations Personnel
Contract Services Providers
Emergency/Disaster
Management Students

Now more than ever,
IAEM is for you...

IAEM brings together emergency managers and disaster response professionals from all levels of government, as well as the military, the private sector, and volunteer organizations around the world.

- Largest expert network offering solutions, guidance and assistance.
- Job opportunities — extensive online compilation.
- Unified voice on policies and legislation.
- Information updates: monthly newsletter and e-mail notifications.
- Professional tools and discussion groups on www.iaem.com.
- Certified Emergency Manager® and Associate Emergency Manager programs.
- Scholarship program.



Join IAEM Today!