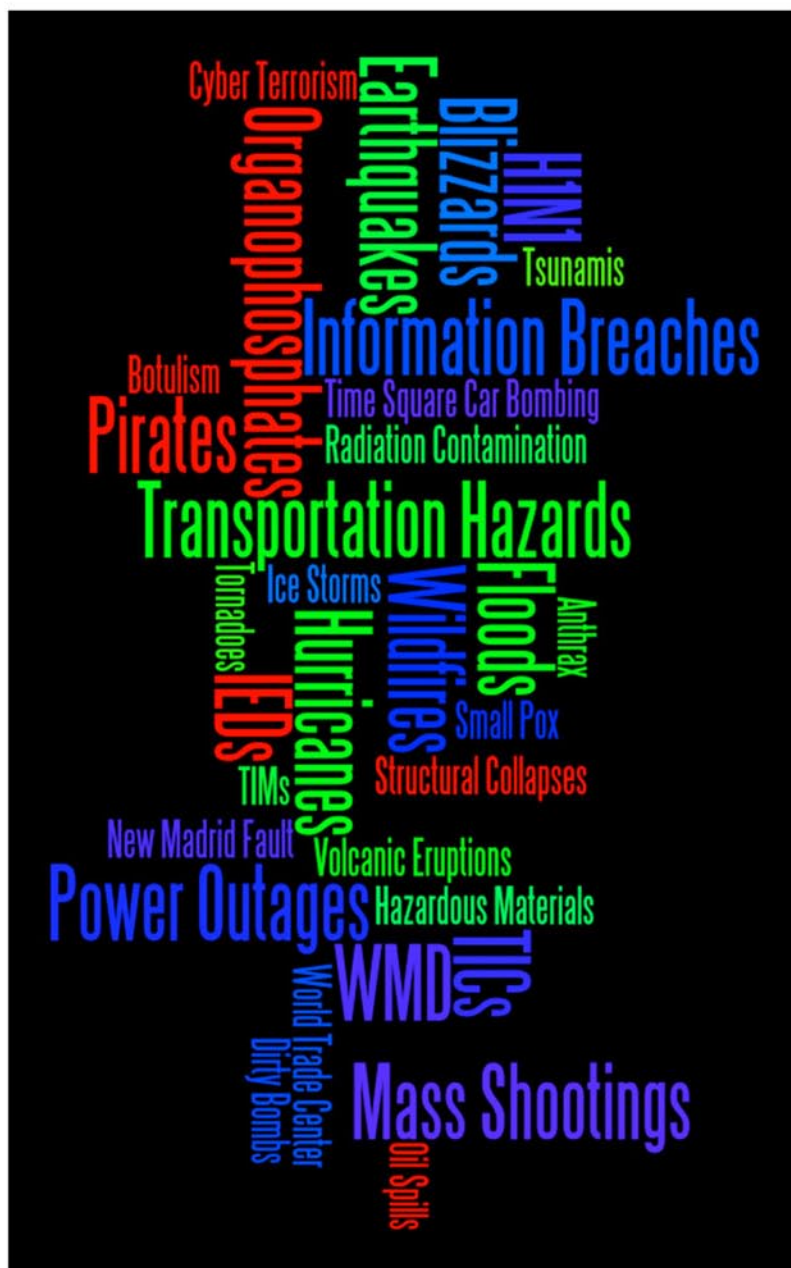




Vocabulary Of Preparedness



PTSD: Its Causes, Effects & Possible Strategies
By Joseph Cahill, EMS

Public Health Emergency Resilience:
The Next Challenging Step
By Bruce Clements, Public Health

The Missing Leg of a
Well Balanced Facility Security Platform
By Joseph Trindal, Law Enforcement

Pre-Exposure Anthrax Vaccination:
A Horse & Cart Situation?
By Thomas K. Zink, Viewpoint

Private Sector Language:
Resilience & the Supply Chain Element
By Dennis R. Schrader, CIP-R

Disaster Resilience:
An Emergency Manager's Perspective
By Kay C. Goss, Emergency Management

The Three "T"s of Terrorism -
Finding the Facts in the News
By Jordan Nelms, Viewpoint

USCG's Small-Vessel
Security Strategy Ready to Launch
By Corey D. Ranslem, Coast Guard

Storm Warnings:
Communications And Utility Resilience
By Omar Alkhalaf, Viewpoint

Air National Guard
Resumes Live-Saving CCATT Mission
By Ellen Krenke, National Guard

Georgia, California, Kansas, and Colorado
By Adam McLaughlin, State Homeland News

The Sentinel XL™ CBRN Difference

The Only PAPR With:

- CAP 2 NIOSH CBRN approved
- Converts to/from CBRN to P100
- Unique backpack
- Alkaline battery pack option
- “Lay Flat” butyl hood
- No fit testing required

*Why Trust Your Life
To Anything Less?*



ILC DOVER
creating what's next»

Ph: 302.335.3911 | 800.631.9567

www.ilcdover.com | customer_service@ilcdover.com

One Moonwalker Rd, Frederica, Delaware, USA 19946-2080

Editor's Notes

By James D. Hessman, Editor in Chief



Federal and state budget plans, bloody riots and peaceful demonstrations, and new attacks by pirates in the waters off Somalia – all have been covered at length in the print and broadcast media in recent weeks, and all are examined somewhat more closely, by emergency-responder professionals, in this monthly “roundup” issue of DPJ.

Most of the pirate attacks that have attracted so much attention in the past several years have taken place in the waters off Somalia, so are of minimal concern to the United States – right? No, just the opposite, says Corey Ranslem, who points out that it would be extremely difficult if not impossible for the U.S. Coast Guard or any other law-enforcement agency to stop and inspect fishing vessels, yachts and/or other pleasure craft (a gambling casino, perhaps?) packed with explosives and coming up the Potomac to Washington, D.C. USCG planners are working on the problem, but have no totally acceptable answer at present.

Thomas K. Zink looks at an even more deadly danger – a possible anthrax attack – and asks: (a) Why has an effective U.S. anti-anthrax policy not yet been implemented? And (b) Why are so many doses of anti-anthrax vaccine (500,000 a year or thereabouts) being wasted so casually?

Three other equally distinguished authors look at important but as yet unresolved policy issues. Bruce Clements begins with an analysis of Homeland Security Presidential Directive 21 (HSPD 21), the National Health Security Strategy (NHSS), and the Biennial Implementation Plan (BIP) and suggests, reasonably enough, that all three of these foundational documents should not only be explained more clearly to the American people but also implemented more expeditiously. Joseph Trindal points out that the U.S. strategy for “facility security” focuses primarily (almost exclusively, in fact) on risk assessments, the planning of security measures, and the implementation thereof. There should be a fourth leg of that strategy, he says: periodic testing, and follow-up training. Dennis Schrader rounds out the policy review by noting that the private sector and numerous government agencies are united in their support of Supply Chain Logistics (and other abstractions) but have yet to develop, and use, a common language in their planning papers and public discussions.

Kay Goss relieves the tension considerably in her review of recent improvements – at all levels of government – in disaster resilience capabilities. Jordan Nelms provides several cogent clues (based on Targets, Tactics, and Technology) that everyday citizens can use to learn “the true facts” behind the typically unfathomable media reports, and official statements, on recent acts of terrorism. Omar Alkhalaf tells how the lessons learned from the destructive weather storms in Iowa (in 2007) and New Hampshire (in 2008) have been used to improve disaster planning in not only those states but in many others as well. Joseph Cahill discusses PTSD (post-traumatic stress disorder) and points out that it is common not only among service personnel but in the ranks of emergency responders as well. Ellen Krenke adds a bullish report on the use of National Air Guard units for Critical Care Air Transport Team missions. And the ubiquitous Adam McLaughlin rounds out the issue with encouraging reports on recent milestone homeland-security events in the Great States of California, Colorado, Georgia, and Kansas.

About the Cover: Imaginative WordDoodle by DPJ staff artists provides a handy visual reminder of some but by no means all of the horrendously efficient dangers facing Americans and their Free World allies in the Brave New World of the 21st century.

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:

Bruker Detection

Disaster Response & Recovery Expo

Environics

FLIR Systems Inc.

Idaho Technology Inc.

ILC Dover

International Hazardous Materials
Response Teams Conference

PROENGINE Inc.

Upp Technology Inc.

© Copyright 2011, 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.





REDUCING THE SECURITY BURDEN WITH PROVEN TECHNOLOGIES

Major sporting events bring together hundreds of thousands of people to a single location, presenting new and unique security concerns that must be overcome. Such new threats require new thinking. From crowd management tools like the SkyWatch to handheld explosives detectors like the Fido, FLIR provides proven tools for extraordinary event security.

www.flir.com/detection

 **FLIR**[®]
Extraordinary Protection

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

PTSD: Its Causes, Effects, and Possible Strategies

By Joseph Cahill, EMS



PTSD or Post Traumatic Stress Disorder is the term used to describe the human reaction to an overwhelmingly stressful experience. PTSD manifests itself in many ways, including: (a) an avoidance of family, friends, or colleagues, even human contact in general; (b) a constant feeling of being threatened and a parallel need to be wary; and (c) intrusive images and/or flashbacks. These symptoms impair the sufferer's ability to function, and can persist for a month or so, and sometimes much longer.

The general public first became aware of PTSD when it was publicized as a common disorder affecting military combat veterans. Less well known is the fact that many first responders also suffer from the disorder. When faced with overwhelming events, members of the nation's general population at large also can suffer from the disorder.

Although some events, such as the 9/11 terrorist attacks, are so overwhelming that they can be anticipated to cause PTSD, various "routine" incidents may also cause PTSD, as can the cumulative stress developed from months or even years of emotionally harrowing events – which is usually why it affects first responders.

Social Support, Internal Strength And the Exercise of Common Sense

Resilience is the term used to describe the cumulative factors that allow an individual to continue to function in spite of facing severely stressful events on a continuing basis. Those factors include but are not limited to such internal strengths or characteristics as personal competence, a tolerance of negative results, the positive acceptance of change, and individual spirituality; also some external features such as the social support provided by family and friends. The combination of these factors is believed by many if not all psychiatrists to improve the individual's ability to cope not only with stress in the short term – during a specific incident, for example – but also with the aftereffects of stress, including PTSD, in the long term.

Many of the factors that create or strengthen the resilience of an individual are his or her personal choices – that person's spirituality and religious beliefs, for example – and cannot (and should not) be dictated by an employer. However, it is possible to encourage spirituality by accommodating employees' work schedules so they can attend services and/or pursue their faith in other ways; this must be done, of course: (a) without promoting any particular faith; but also (b) by establishing and adhering to a zero-tolerance policy for those who may be tempted to ridicule or discourage another's faith.

Promoting physical exercise – on the job, if and when necessary – is another step the employer can take that will improve the resilience of individual members of the responder team. Installing workout equipment or allowing on-duty time to exercise

may seem to some, of course, like an extravagance; however, a reasonable and properly planned workout program has a payout on many levels, including the probable (but difficult to quantify) reduction of PTSD symptoms by a reduction in overall individual and team stress.

Leaders, Peers, and Professional Help

Here it is worth noting, and emphasizing, that fostering a corporate culture that supports the individual employee and helps build a social structure that is also supportive – and that does not allow intolerance in either the pre-event or post-event time periods allocated – may decrease the impact of stressful events.

Coaches, psychiatrists, and other health care professionals credit the support of one's peers as an invaluable asset not only for the individual but also for that person's team (or other social structure). Respected senior staff members are usually the ideal leaders, and examples, for peer support teams; however, they themselves have to believe in what they are doing. Any staff member, no matter how highly respected otherwise, who is required (another way of saying forced) to assist in building peer support will seldom if ever be as effective as another member of the same team who truly believes in what he or she is doing.

Finally, there must be strong support, from mental health specialists, for those who continue to suffer from the disorder. Ignoring it can and often will lead to loss of staff – or, worse, to staff suicides. It must be recognized, moreover, that there are some sufferers who need more support than the team leader, or employer, can directly provide – in which case those suffering from PTSD must be referred to professionals who are able to provide greater in-depth help.

To briefly summarize: As long as there are courageous men and women able and willing to step into the line of fire and cope with extreme events, personally shouldering the stress of saving others – and at times trying, *unsuccessfully*, to save others – there will continue to be cases of PTSD. The United States has the obligation, as a society, and the first responder community

has the same obligation, as a true band of brothers (and sisters), to provide the support those men and women need and thereby remove all stigma from this terrible disorder and the treatment it requires.

Your Opinion Matters! DomPrep is conducting a brief survey on PTSD; if you or someone you know has ever experienced PTSD, your feedback is greatly appreciated. Take Survey! (<http://www.surveymonkey.com/s/ptsd11>)

The general public first became aware of PTSD when it was publicized as a common disorder affecting military combat veterans; less well known is the fact that many first responders also suffer from the disorder [and] when faced with overwhelming events members of the nation's population at large also can suffer from the disorder

For additional information

<http://theklaxon.com/ptsd-treatment-a-necessity-for-military-civilian-first-responders>

http://www.armytimes.com/news/2007/09/ap_ptsd_070901/

<http://ajp.psychiatryonline.org/cgi/content/abstract/147/6/729>

http://missoulia.com/lifestyles/health-med-fit/article_3af8cab8-d8c2-11de-9cad-001cc4c03286.html

9-11 PTSD study

<http://aje.oxfordjournals.org/content/early/2010/12/28/aje.kwq372.full?sid=763db533-7b21-4e24-8de0-ac4b-69283be5>

PTSD story about Aspen SAR staff member
<http://ohsonline.com/articles/2011/01/04/first-responder-ptsd-story-opens-debate.aspx>

Resilience research

<http://www.med.navy.mil/sites/nmcscd/nccosc/healthProfessionals/Documents/Resilience%20TWP%20formatted.pdf>

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. He also served for five years as the citywide advanced life support (ALS) coordinator for the FDNY - Bureau of EMS, and prior to that was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem. Much in demand as a speaker – he has addressed venues as diverse as the national EMS Today conferences and local volunteer EMS agencies – Cahill also served on the faculty of the Westchester County Community College's Paramedic Program and has been a frequent guest lecturer for the U.S. Secret Service, the FDNY EMS Academy, and Montfiore Hospital.

Public Health Emergency Resilience: The Next Challenging Step

By Bruce Clements, Public Health



Homeland Security Presidential Directive (HSPD) 21, which focuses on Public Health and Medical Preparedness, was issued in October 2007. It articulated the current administration policy on the strategic direction and focus of public health preparedness in coming years. HSPD 21 also focuses on four key components of public health and medical preparedness in particular: bio-surveillance; countermeasures distribution; mass-casualty care; and community resilience. The first three have been hallmarks of public health preparedness since the initial surge of funding and public interest in the nearly ten years that have passed since the 2001 terrorist attacks.

The key components of preparedness programs are therefore well understood – even though some associated definitions and measures of certain preparedness components continue to be debated. However, among the four components described by HSPD-21, community resilience seems to be the least understood and most poorly defined.

The two key documents issued since HSPD-21 to clarify, elaborate, and explain the operational implementation of this policy are the National Health Security Strategy (NHSS, issued in December 2009) and the Biennial Implementation Plan (BIP, issued in July 2010). The NHSS focuses on the general activities and outcomes needed to move the nation toward the strategy, and the BIP provides a roadmap for the next two years to move the nation toward health security – which, as spelled out in these documents, define health security as follows:

National health security is achieved when the Nation and its people are prepared for, protected from, respond effectively to, and are able to recover from incidents with potentially negative health consequences.

In order to create this complex health security framework, two goals are established: (a) building community resilience; and (b) strengthening and sustaining health and medical emergency response systems. Those involved in managing these programs have done an outstanding job in developing the federal, state, and local health and medical preparedness and response infrastructures. Over the past decade, the Centers for Disease Control and Prevention (CDC) provided over \$7 billion for the Public Health Emergency Preparedness Program (PHEP).

In addition, over \$3 billion has been allocated by the Department of Health and Human Services (HHS) for the Hospital Preparedness Program (HPP). The infrastructure and capacities established through these programs form the foundation of the proposed health security framework. Today, the new challenge is orchestrating these systems and capabilities into the resilient, coherent, and functional framework suggested in HSPD 21 and the follow-on documents mentioned above.

Public Health Preparedness And Community Resilience

The methods used to measure public health preparedness have evolved in recent years and continue to be the focus of considerable debate. In addition, the term “community resilience” has become even more challenging to define and measure. The NHSS suggests that community resilience is predicated upon healthy individuals who have an informed understanding of preparedness – and of the resources needed to care for themselves in times of emergency. The resulting resilience also requires a fundamental inter-connectedness of individual citizens, both in their neighborhoods and in their extended community, to facilitate the sharing and balancing of available resources. This community connectivity is sometimes referred to as social capital. However, measurement of this preparedness prerequisite is complicated by the vagueness of the social capital concept itself.

It seems ironic that, in this new age of social networking tools such as Facebook and Twitter that individual citizens are often less connected to others living in the same general geographic area than ever before. Use of the new Internet tools is an excellent way to keep in touch with others across the country and around the world. However, these connections are often based more on common interests than they are on zip codes. One result is that, although on-line “communities” continue to rapidly expand, people living in closer geographic proximity to one another often have less interaction. However, direct connections with one’s neighbors can still make a major and even life-saving difference during emergencies.

This is especially true for the most vulnerable populations – e.g., elderly residents living alone who lack a personal support structure, including nearby friends and family members. This deficiency in social capital represents a cultural shift in recent decades that poses ongoing challenges to the assurance and sustainment of community resilience when the community is facing major public health emergencies.

Public Health Preparedness And Systems Resilience

The concept of resilience is not limited to the sum total resilience of individual citizens, their families, and their communities. It also includes the robustness and interconnectedness of public health and healthcare systems. While these systems have achieved tremendous progress in preparedness over the past decade, efforts are still hampered by unstable funding “silos.” When these systems operate in such silos it creates a lack of connectivity that precludes resilience. If anything goes wrong with a single system, therefore, failure may well have a domino effect that causes needed systems to collapse like a house of cards amidst critical operations.

Truly resilient preparedness systems are robust, interconnected, and redundant. They also must be able to leverage public/private partnerships. No single government program or system can achieve resilience on its own. Nor can any private system, including those run by non-governmental organizations (NGOs), operate autonomously with true resilience. A sound public health emergency response system must include private organizations, as well as public agencies at the local, state, and federal levels of government. They must work in harmony to optimize resilience.

A resilient public health preparedness infrastructure may be cultivated only by focusing on the three core public health functions: Assessment; Policy Development; and Assurance. These public health systems are guided by rigorous epidemiological **Assessments** to focus resources on health threats. They are implemented through effective **Policy Development** that is built upon rigorous science translated into practice. Finally, they are **Assured** by continuous evaluation that ensures improvements are identified through after-action reviews from actual emergencies, as well as exercises and drills. Improvements are incorporated into future plans and training and the process is repeated. The nurturing of public health preparedness system resilience requires that these core functions be orchestrated across multiple layers of governmental and non-governmental stakeholder agencies.

Unfortunately, the systems described are often lacking throughout the United States. There are still no interoperable electronic health and medical intelligence systems available to provide real-time situational awareness. Moreover, research, although necessary in the development of sound preparedness policy, is not funded under the primary public health and medical preparedness funding streams (PHEP and HPP). There is also a tendency across all of these systems to focus on preparedness and response – but with little effort toward community recovery. Obviously, resilient systems must expand their focus to include long-term recovery efforts that are often left for the NGOs mentioned earlier.

A Few Remaining Questions Related to Emergency Resilience

A resilient community and public health system limits the impact and/or stress of an emergency and facilitates a rapid recovery. Individuals, families, and communities with an established level of preparedness are better able to respond effectively and to withstand the health impact of a disaster. They are also able to return more quickly to normal. Moreover, communities with greater social capital are able to leverage their interconnectedness to help compensate for those less able to prepare, respond, and recover. However, the role of government in expanding community resilience is still not well understood.

That lack of understanding raises several public policy questions, including the following: (a) Should local, state, and federal agencies play a role in enhancing person-to-person and community-to-community relationships? (b) If so, how much control should be exercised? (c) Should government play a facilitating role? (d) After these roles have been defined, what programs or processes may be instituted to develop community resilience?

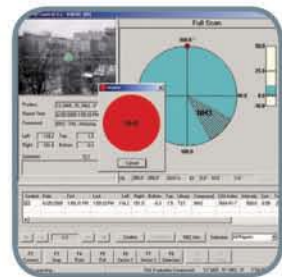
There has been very little published to date, it seems, that would adequately answer these and other critical questions. Fortunately, though, a synergistic environment of public health emergency resilience usually does result when a resilient community is supported by a similarly resilient health and medical infrastructure. Health and medical systems of the future must be prepared to meet anticipated as well as unanticipated challenges. The goals and strategies described in the key foundational documents mentioned earlier are a major step in a new direction. The only way to meet these challenges is by intentionally building and strengthening public health and healthcare partnerships based on clear definitions, quality measures, and systematic evaluations. To achieve all this will require not only more succinct guidance from the funding agencies involved but also additional resources. These resource needs are unlikely to be met in the near future given current budget shortfalls. Today, most federal agencies and the programs they fund are being asked – as are the American people – to do more with less. Given the challenging vision for the future of public health preparedness, one can only hope that the value of this infrastructure and the need for this resilience is established as a necessary and continuing priority.

*Bruce Clements is the Public Health Preparedness Director for the Texas Department of State Health Services in Austin, Texas, and in that post is responsible for health and medical preparedness and response programs ranging from pandemic influenza to the health impact of hurricanes. A well known speaker and writer, Clements also serves as adjunct faculty at the Saint Louis University Institute for BioSecurity. His most recent book, *Disasters and Public Health: Planning and Response*, was released in 2009.*

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

The Missing Leg of a Well Balanced Facility Security Platform

By Joseph Trindal, Law Enforcement



The protection of high-value properties, and of the people working and/or living within them, is an important and challenging task. However, those responsible for most of the nation's facilities typically invest in only three legs of the site security platform – i.e., those broadly related to risk assessments, planning, and the implementation of security measures. For that reason, although a site's security profile may look stable and function well under normal use, this “three-legged” approach in protection is inherently flawed in design – guarding primarily and sometimes only against the threat characteristics determined in the facility's risk assessment.

Nonetheless, U.S. protective practices and technologies have evolved in response to catastrophic events such as the 1995 bombing of the Alfred P. Murrah Federal Building in downtown Oklahoma City, the 1998 bombings of U.S. embassies in Kenya and Tanzania, and the bungled 1993 truck bombing of the World Trade Center in New York City.

Public buildings that were “open access” in the 1990s are now much better designed – and equipped with multiple layers of security protective measures. But the effectiveness of those measures is inconsistent, and varies considerably from one location to another. The end result is that, despite all of the human capital and financial investment in planning, implementation, and staffing that has been used to improve security in recent years, many dangerous gaps remain – and should be faced head-on. Particularly important is the fact that, whether the security measures now in place are technological or human in nature, they must be tested, thoroughly and frequently, to ensure their effectiveness.

Functional Security Testing Models

Functional security testing models can range from those using a very soft approach, such as informal procedural knowledge assessments, to the “hard penetration testing” described by former U.S. Navy SEAL Richard Marcinko in his 1992 best-seller *Rogue Warrior*. Any functional security testing model should assess the performance of not only security equipment but also security personnel under actual operating conditions. Moreover, all functional security testing should be well planned, with clear objectives

set that: (a) link to predetermined threat modalities; and (b) incorporate measurable performance benchmarks.

In addition, functional security test findings, regardless of the model used, also should be well documented – and then incorporated in an improvement action plan approved by any agency or collection of agencies (a Building Security Committee, for example) responsible for improving security.

Here it should be noted that functional security testing usually differs considerably from the preparedness-exercise models used. The most significant difference is that testing is almost always unknown to the person or group being tested. Exercises, even functional exercises, depend more on artificiality than functional testing does. There are a number of similarities between the two as well.

As in operational exercises, *safety* is and must be the first priority in functional security testing. The planning and preparatory processes are fairly similar, except that there is no artificiality of location, communications, or preparation by those tested. The after-action briefing can be and frequently is very similar to those used in exercises – and the improvement action planning and implementation should be identical.

A very soft testing could involve inquiries of personnel related to the security and emergency procedures used in various situational scenarios. This approach can and should be as simple, for example, as asking security personnel *and* employees the basic question “What would you do if [etc].” This approach can be both spontaneous and unobtrusive, but also quite effective, when applied to security entrance points. For employees, it can and should test the depth of their understanding of facility emergency procedures.

A Broad Spectrum Of Reasonable Alternatives

Other functional security testing models might and probably should involve the use of deceptive or surreptitious penetration attempts to facilities – and/or to supposedly secure areas within those facilities. The testing methods used should involve security personnel and employees in different tests. One com-

mon access-control vulnerability is so-called “tailgating” – i.e., when an authorized person allows someone to follow him or her into a secure area without challenge and authorization verification. This vulnerability is relatively easy to test and correct – if proper procedures are demanded and enforced.

Many other testing methods also can be used. Testing the detection of and response to dangerous and prohibited items – firearms and IEDs (improvised explosive devices), for example – should always be very carefully monitored. Fortunately, there are a number of zinc-constructed training firearms that have the look, feel, function, and detection image characteristics of real firearms, but are not capable of accepting a live cartridge.

Other simulation devices are readily available as well – but must be used with common sense. The IEDs used in testing should be well marked as “INERT.” Also, the testing methods designed to generate a “contain and secure” response should be carefully controlled as well. The U.S. Marshals Service of the Department of Justice routinely prepositions a sworn deputy or two in close proximity to the screening point in order to control and terminate the test after the detection and appropriate response by security personnel have been achieved.

Aggressive “hard site” testing should be limited to those high-risk/high-value sites in which security personnel are trained, equipped, and procedurally prepared to execute highly predictable response actions. Hard red team testing – i.e., actual attempts at physical site penetration – should be limited to a relatively small number of facilities.

Narrowing the Gap Through Improvement Action Planning

The full investment in security testing needed can be achieved only through improvement action planning and implementation. Testing may reveal gaps that can be narrowed or perhaps even eliminated by training, procedural revisions, repositioning, and/or recalibrating security equipment as well as improving communi-

cations capacities. Improvement action planning and implementation should focus, therefore, on strengthening the security posture of the site rather than on correcting the failures of a single individual.

Obviously, functional security testing may in fact reveal individual performance deficiencies, but those should be addressed as a supervisory corrective issue within the site’s own human-resources procedures. Conversely, positive performance in functional security testing can be linked

to incentive programs that elevate, and appropriately reward, motivation, dedication, and vigilance.

Like the exercises, functional security testing should be a recurrent part of the individual site’s overall security program. For that reason, the “best practices” models for all-hazards preparedness should incorporate a clearly defined preparedness exercise cycle. A best practice for functional security validation should also include a recurrent cycle for testing and evaluating various aspects of the site’s security profile.

To briefly summarize: Functional security testing is a vital, important, and absolutely essential aspect of a truly comprehensive, and therefore effective, security program. Just as a table is much sturdier when it rests on four legs instead of three, the security and emergency

preparedness posture of a critical-infrastructure site is much stronger when recurrent functional security testing and improvement action planning are meticulously planned, and used effectively.

Public buildings that were “open access” in the 1990s are now much better designed – and equipped with multiple layers of security protective measures – but the effectiveness of those measures is inconsistent, and varies considerably from one location to another

Joseph Trindal is the managing director at KeyPoint Government Solutions Inc., he is in charge of the company’s Infrastructure Protection Services. He also serves on the Board of Directors at InfraGard Nation’s Capital Member Alliance. Trindal retired in 2008 from the U.S. Department of Homeland Security, where he had served as Director for the National Capital Region, Federal Protective Service, Immigration Customs Enforcement. In that post, he was responsible for the physical security, law enforcement operations, emergency preparedness, and criminal investigations of almost 800 federal facilities in the District of Columbia, Northern Virginia, and suburban Maryland. He previously served, for 20 years, with the U.S. Marshals Service, attaining the position of Chief Deputy U.S. Marshal and Incident Commander of an Emergency Response Team.

CHEMPRO

Fixed Chemical Detector

FX

The ChemProFX is a permanently mounted gas and vapor detector that provides continuous 24/7 protection of fixed infrastructure from the threat of Chemical Warfare Agents (CWAs) and Toxic Industrial Chemicals (TICs). It has industry-leading sensitivity and false alarm rejection in the most user friendly and low-maintenance package in its class.



- Low life-cycle costs & logistics
- Predictable maintenance
- Easily mounted and interfaced
- Industry leading sensitivity



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

Pre-Exposure Anthrax Vaccination: A Horse & Cart Situation?

By Thomas K. Zink, *Viewpoint*



Local civilian emergency professionals who react to *all* “suspicious powder” events – e.g., police/sheriffs/security officers, firefighters, and emergency medical technicians (EMTs)/paramedics as well as members of hazmat and SWAT teams – are not currently immunized against anthrax. But personnel in what might be called “the second wave” of WMD (weapons of mass destruction) responders – i.e., the members of the nation’s Civil Support Teams (CSTs), which are summoned to only a fraction of such events – *are* vaccinated.

This contradictory order of priorities is not only confusing but also becomes indefensible when one considers the monthly waste of 500,000 expiring doses of anthrax vaccine from the Strategic National Stockpile (SNS). However, there seems to be a growing consensus that now is the time to begin administering the safe, effective anthrax vaccine to emergency responders before exposure/infection.

Since the 11 September 2001 terrorist attacks against the United States there have been numerous improvements in homeland security planning efforts at all levels of government – state and local as well as national. A common theme throughout these strategic plans is the emphasis on response. However, there also are signs that U.S. government officials are striking a more balanced approach between post-attack response and pre-event preparedness. In 2010, for example, the U.S. Centers for Disease Control and Prevention (CDC) published recommendations on use of the anthrax vaccine that support the voluntary pre-event vaccination of emergency responders.

Unsubstantiated Rumors And Irrelevant Calculations

Nonetheless, one year later, hesitancy prevails – possibly because of the mistaken belief of some critics that the risk of an anthrax attack is incalculable (or nil) and/or has been fueled by the rumor – unsubstantiated – that the vaccine itself is unsafe. When considering risk, though, anthrax bioterrorism is not, and should not be considered as, a communicable disease. It is not productive, therefore, to apply the customary epidemiological calculations on risk of infection and impact of immunization – i.e., the force of infection, basic and effective reproductive numbers, average age of those infected at the time of infection, and inter-epidemic period – to an anthrax attack. Instead, anthrax bioterrorism is more logically, and more effectively,

assessed as a threat that can and should be calculated as a function of three variables: (a) the probability of danger; (b) the existence of vulnerability; and (c) the degree of impact.

Numerous credible studies and analyses agree that the probability of an anthrax attack is real and continuing. In December 2008, for example, the bi-partisan Commission on the Prevention of WMD Proliferation and Terrorism stressed the importance of enhancing the nation’s capabilities for rapid response to prevent a biological attack – particularly one in which anthrax would be the terrorists’ weapon of choice. On 21 October 2009, the Commission restated its concerns and asserted that anthrax is the most likely near-term threat.

As is stipulated in the U.S. Army’s AVIP (Anthrax Vaccine Immunization Program) plan, the anthrax threat provides the rationale for the routine administration of the anthrax vaccine to U.S.-deployed Department of Defense (DOD) personnel and members of the National Guard’s Civil Support Teams. An additional rationale, if such is needed, is the nagging fact that the United States has already suffered – in the immediate aftermath of the 11 September terrorist attacks – a covert, multi-site, multi-tier, lethal anthrax attack that killed five people, infected or otherwise affected thousands of others, and cost American taxpayers hundreds of millions of dollars.

A Clear and Significant Danger

The current level of vulnerability to anthrax is significant. On 11 December 2002, the *Journal of the American Medical Association* reported that weaponized anthrax powder quickly dissipates into the invisible, odorless, tasteless, gaseous phase and is easily re-aerosolized. Identifying what might be considered a “safe zone” is very difficult, and the personal protective equipment (PPE) currently available is not fool-proof. Six responders to the post-9/11 anthrax attacks were infected, for example, while inspecting the Hart Senate Office Building despite the fact (as was reported in January 2007 by the *Journal of Infectious Diseases*) that they were wearing hazmat suits at the time.

Of even greater importance is the fact that – as reported in the August 2001 *International Journal of Antimicrobial Agents* and again in the August 2004 *Journal of Antimicrobial Chemotherapy* – anthrax can be made resistant to all currently stockpiled antibiotics. Vulnerability is at its greatest in an attack using strains of anthrax that are resistant to the antibiotics currently

stockpiled. In this scenario, post-exposure antibiotics afford no protection, and post-exposure vaccine cannot be expected to confer immunity quickly enough to prevent infection.

In terms of the potential impact of a major anthrax attack, a 1970 World Health Organization (WHO) expert committee estimated that an aircraft release of 50 kg of anthrax over an urban population of five million people would result in 250,000 deaths – 38 percent of whom would die without treatment; in addition, another 125,000 people would be severely incapacitated. In 1993, the U.S. Congressional Office of Technology Assessment confirmed the original WHO data. More recent modeling – e.g., the mathematical model published in 2003 in the *Proceedings of the National Academy of Sciences* – puts the lethal capability of weaponized anthrax as equivalent to that of a nuclear bomb – but without the same property damage.

From an economic perspective, the CDC developed a model suggesting that it would cost an estimated \$26.2 billion per 100,000 persons to treat those exposed in an anthrax attack. On 7 March 2002, the *Washington Post* reported that the decontamination, mentioned above, of the Hart Senate Office Building following the 2001 anthrax attacks took several months and cost approximately \$23 million. A follow-up *Post* article, on 18 December 2002, reported that the decontamination of the two postal facilities attacked – one in the Brentwood area of the nation’s capital; the other in Hamilton Township, New Jersey – required more than a year of intense remediation and cost in excess of \$100 million. When one considers that, according to the *Proceedings of the National Academy of Sciences*, the amount of anthrax involved in the contamination of each of these facilities was probably less than 1 gram, it immediately becomes obvious that the cost/benefit ratio is totally on the side of the terrorists.

Accusations vs. Evidence – Plus a Clear Need for Speed

Another stumbling block frequently encountered is the unscientific accusation sometimes made that the anthrax vaccine now available is unsafe. Those who make this charge, though, ignore the abundant evidence to the contrary that is easily available. In a 2008 article published in *Clinical Infectious Diseases*, for example, J.D. Grabenstein (former executive director of the Army’s anthrax immunization program), cites over 20 human studies that have assessed the safety of anthrax vaccination and found not only no unusual or unexpected patterns of adverse events but also no deaths and/or serious long-term adverse events.

Moreover, the anthrax vaccine has been determined safe for its intended use by, among other agencies and organizations: the U.S. Food and Drug Administration; the Armed Forces Epidemiology Board; the Anthrax Expert Vaccine Committee; the Institute of Medicine; and the CDC Advisory Committee on Immunization Practices. In addition, according to the Institute of Medicine, the safety profile of the anthrax vaccine is similar to that of other adult vaccines – e.g., influenza and hepatitis A & B – now available.

Statistics can be and frequently are manipulated, of course, but it is difficult to ignore two statistics of overwhelming magnitude – namely, that: (a) the anthrax vaccine has been safely used for at least 40 years; and (b) more than 10 million doses of this vaccine have been administered to over three million people.

Moreover, in one landmark safety study published in 2002, the U.S. Anthrax Vaccine Expert Committee (AVEC) exhaustively reviewed complete data on almost 1,350,000 doses that had been administered to over 400,000 subjects. According to the AVEC study, the “adverse event” rate was 1 in 2,500 injections, and the “serious adverse event” rate was 1 in 200,000 injections – none of which were fatal, life-threatening, or caused permanent disability. Here it is relevant to note, to put the adverse-event risk into an even clearer perspective, that U.S. Census data place the odds of a fatal auto accident at 1 in 98 for a person living in the United States who reaches the age of 80.

To briefly summarize: the anthrax threat is real and continuing. The vaccine solution is well known, safe, effective, and already available – but most of it is going to waste. The time is *now*, therefore, to put the vaccination “horse” in front of the “cart” of preparedness and protect the local civilian emergency responders upon whom the community relies for its own protection and resilience.

Dr. Thomas K. Zink is an independent healthcare and biodefense consultant and an adjunct associate professor of community health at Saint Louis University. He practiced and taught emergency medicine for over a decade before shifting his focus to health system quality improvement, illness/injury prevention, immunization policy and practices, and biodefense. As both a consumer and an industry advocate, he was the driving force in building consensus for the U.S. policy of universal childhood vaccination against hepatitis A and in achieving a global recommendation to booster adolescents and adults against pertussis. He is also: the founding Director of Project Equal Immunization Policies and Practices (EQUIPP) – an initiative to improve vaccination protection in emergency responders; a retired Diplomat of the American Board of Emergency Medicine; a past Fellow of the American College of Emergency Medicine; and a licensed Physician & Surgeon rated in “Good Standing” by the Missouri State Board of Healing Arts.

Private Sector Language: Resilience & the Supply Chain Element

By Dennis R. Schrader, CIP-R



The theory that public-sector agencies should rely on the private-sector resilience of owners/operators of critical infrastructure as a disaster-recovery strategy is both valid and useful. The question, though, is this: How does or should that reliance work in the real world? Unfortunately, it can be a chicken-or-egg scenario – i.e., what comes first, the resilience or the reliance?

One possible path to the correct answer is for the public sector to learn the language of the private sector and adapt it to the public sector. Here, what is described as Supply Chain Logistics would be a key element in the overall resilience equation that could be both a logical and a viable place to begin.

The reality, of course, is that the private sector already practices resilience every day – but its “language of resilience” involves and is focused primarily on such terms, and priorities, as “Risk Management,” “Business Continuity,” and the previously mentioned “Supply Chain Logistics.”

The government uses the same, or similar, concepts, but for very different purposes – because government agencies are more concerned, understandably, about responding to and recovering from incidents – which, everyone hopes, will be rather infrequent – that entail higher-priority public-safety considerations. The private sector is concerned, of course, about Supply Chain performance, which is the key to maintaining not only customer satisfaction but also cash flow – both on a daily routine basis and in a crisis situation as well.

In federal language, the National Incident Management System (NIMS) Resource Management Component is the key doctrine used in providing disaster logistics capabilities in times of emergency. The foundation of that component is the principle of using “Mutual Aid” arrangements as the prerequisite for support. What is called an Emergency Management Assistance Compact (EMAC) is a key element of state-to-state mutual-aid agreements – which developed, incidentally, from a Southern Governors Association initiative in the early 1990s.

EMAC and the Request/Disaster Sequence

The EMAC/mutual-aid system relies heavily on reimbursement from the federal government – *after* a disaster has been officially declared. After such a federal declaration is made, of

course, the Federal Emergency Management Agency (FEMA) begins to coordinate the federal resources needed – but only as and when requested by the states affected by the disaster.

Unfortunately, it is not always clear exactly how (and/or when) the private sector can or should plug into this federal doctrine to obtain the resilience capabilities needed. One very interesting approach might be to employ the Supply Chain Operations Reference (SCOR) developed by the Supply Chain Council (SCC – an independent non-profit organization of about 1,000 private-sector companies and corporations). The SCOR was originally developed by PRTM, a private-sector management consulting firm, to organize its multi-company benchmarking studies. SCOR analyzes five high-level processes – grouped under such generic terms as Plan, Source, Make, Deliver, and Return – in a model that follows a logical three-part sequence: Business Process Re-engineering; Benchmarking; and Best-Practice Analysis.

Agencies and jurisdictions could document their existing Disaster Logistics systems and processes and benchmark them to determine the performance measures of the current disaster-logistics model. By comparing existing systems and processes to those spelled out in best practices, capabilities gaps could be identified, after which the improvement plans needed could be developed – and then implemented with all deliberate speed.

There is an additional benefit that can be derived from understanding the private-sector models – namely, that the government could more easily, and more quickly, identify specifically where and how the private sector fits into the Resource Management (i.e., Supply Chain Logistics) Component. Such understanding might lead in turn to: (a) creation of the language and framework needed for an improved private-public sector dialogue; and (b) a valid comparison that would initially coordinate the private-sector supply chains and government resource-management structures essential to improved disaster planning.

Mutual Benefits Plus a Logical Starting Point

The government obviously would benefit by leveraging existing private-sector techniques and, of greater importance, would gain greater credibility by adopting the

private-sector language used in Supply Chain Logistics. Private-sector companies and corporations then could compare their processes to those of the government and thus more easily determine: (1) where they can, and should, play a supporting role; and (2) how they should negotiate their own planned contributions – prior to an actual incident, it should be emphasized.

Of course, the need to agree on such collaboration is easier said than done. For the public sector, adhering to this process would require not only a major change in thinking but also a rather large investment of time and energy to learn the private-sector systems and vocabulary. For the private sector, the same changes would require a reciprocal commitment of resources and time to fully engage the government. However, if the notion of private-sector resilience is to become reality, this type of thinking must emerge – again, as suggested earlier, with all deliberate speed.

It seems clear in any case that, despite the problems and pitfalls that might be encountered, such a change in attitude, and in procedures, is definitely possible. To the public sector's credit, the EMAC is both an elegant and very innovative tool that actually works as it is intended to (despite the fact that it does not usually receive the credit deserved for its effectiveness).

The private sector possesses significant logistics capabilities that can be brought to bear in times of crisis, but those capabilities must be used both efficiently and in accordance with plans that have been developed pre-incident. Nonetheless, in the context of EMAC's successful history, analyzing that system as a model may still be the best starting point for the creation and implementation of other improvements using SCOR.

Captain Dennis R. Schrader, USNR (Ret.), is president of DRS International, LLC, and former deputy administrator of the Federal Emergency Management Agency'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.

Disaster Resilience: An Emergency Manager's Perspective

By Kay C. Goss, Emergency Management



Resilience, as a concept, is still relatively new to the emergency management field. It first appeared in the 1990s, when discussions of disaster resistance, mitigation measures, and risk management were being more fully defined, designed, and discussed by the profession. Today, there are many examples both of best practices and of lessons learned, as well as improved definitions, a more complete understanding, and more effective use.

After the 9/11 terrorist attacks, the protection of critical infrastructure became a flagship concept. As more time passed and there was a dawning realization that the vast amount of critical infrastructure throughout the United States could not be fully protected 24 hours a day, seven days a week – except by the expenditure of astronomical funding amounts – resilience has come to be recognized by many if not all emergency-management professionals as a better practical option that would be more sustainable over the long run as well.

Within the emergency-management field, resilience encompasses a very broad section of tasks and responsibilities, including but not limited to the following topics: preparedness planning; partnership building; education and training; mitigation measures; architectural design; risk management; continuity of operations; continuity of government; homeland security; law enforcement; physical security; emergency medical services; standards, certifications, and accreditation; auditing and assessments; numerous technological systems, equipment, and devices; sustainable development; the protection of critical infrastructure; and the full spectrum of emergency services. In short, the planning, development, and building of disaster resilience is and should be an all-encompassing task that requires the best efforts of every participating professional involved. Here it is worth noting, though, that in times of sudden disaster almost all citizens can serve as immediate responders – in the only slightly restricted sense of assisting their own families, their neighbors, and their local communities.

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

Vulnerability: The Essential Prerequisite

Resilience cannot be fully understood, of course, without first discussing and understanding another somewhat abstract and all-encompassing term: vulnerability, which is primarily a product not only of exposure to hazards but also of a community's capacity to cope with, respond to, and recover from incidents – its resilience, in other words.

Dr. B. Wayne Blanchard, former director of the Federal Emergency Management Agency (FEMA) Higher Education Program, used the word “resilience” as early as the mid-1990s when discussing various mitigation and disaster-resistance measures. Blanchard saw resilience not as a merely helpful abstraction but as a much broader, more concrete, more inclusive, and (of particular importance) probably more useful term, and was one of the first high-level government officials to mention, use, and help define the term.

Quite a few years later – in 2009, to be more specific – the National Institute for Standards and Technology (NIST) moved the word another notch higher on the emergency-management vocabulary scale by publishing its “Standard Methods to Assess the Resilience of the Built Environment Project,” which many professionals consider the forerunner to the development of specific resilience standards. On that point, NIST said the following:

“Improved metrics that show the relative cost effectiveness of alternative combinations of risk mitigation and recovery strategies will be incorporated into draft ASTM [American Society for Testing and Materials] standards, along with models for evaluating losses and assessing disaster resilience. The mechanism for getting these standard metrics into practice is the ASTM Subcommittee on Building Economics. Finished standards will provide the basis for decision support software to be prepared by the OAE [Office of Applied Economics] for evaluating risk mitigation and recovery strategies.”

Gaining Traction – In the Media And With the Public at Large

Also helping to promote the understanding of resilience in specific and concrete terms rather than as an abstraction are: (a) a new publication – the *International Journal of Disaster Resilience in the Built Environment*, launched just last year – which aims to communicate new practical ideas, applications, and details of education and training, thus building the capacity needed for self-sufficiency; and (b) a number of new books.

Prominent among the latter are: *Disaster Resilience: An Integrated Approach*, by Douglas Paton and David Johnston, which fills several gaps in using both sustainability and resilience as practical concepts within the field of emergency planning; and *Designing Resilience: Preparing for Extreme Events*, by Louise K. Comfort of the University of Pittsburgh.

Resilience also is gaining traction on the Internet, both as an abstract concept and as a slightly “glamorous” new buzz word. Eric Holdeman, former King County Emergency Manager and former ICF Emergency Management Consultant, observed, for example, on his “Disaster Zone” blog, that it is very difficult to measure the disaster resilience of a specific political jurisdiction. He also cited a 2010 article (in the *Journal of Homeland Security & Emergency Management*) that focuses on some, but by no means all, of the “disaster resilience indicators” needed for “benchmarking baseline conditions.”

That article, by several researchers – including Dr. Christopher Emrich of the University of South Carolina – makes several cogent points, including the following:

1. *Emergency management programs are only one component of resilience;*
2. *Additional contributing factors include such variables as income, wealth, insurance, social networks, age of population, the functional needs population, social capital, adaptive capacities; and*
3. *Resilience is multi-dimensional.*

Additional Evidence: Local, State, National, International

There is, in addition to the preceding, considerable (albeit still somewhat anecdotal) evidence to support the belated recognition that resilience is no longer simply an abstract academic term but an inescapably substantive – and extremely important – component of a truly comprehensive disaster-preparedness plan. Following are a few random examples, from scores already available, of how resilience has been recognized – in numerous tangible ways – at the local, state, national, and international levels of government:

The Boston Children's Foundation now provides integrated, community-based psychosocial stabilization initiatives that make effective use of various state-of-the-art trauma-specific intervention strategies that have been carefully

2011

International Hazardous Materials Response Teams Conference

PREPARE YOUR TEAM

Register now for valuable education, excellent networking, a great expo and unique hands-on field trips including:

- The DuPont Experimental Station
- The Public Health Laboratory
- A Special Session at the Rail Yard

MAKE SURE YOUR TEAM
IS READY TO RESPOND
REGISTER TODAY!

May 18 - 22, 2011

Exhibits: May 20 - 21

Baltimore Marriott Waterfront
Baltimore, Maryland

Presented by the IAFC



www.iafc.org/hazmat

designed to develop and enhance the personal and disaster resilience capabilities of young people.

The concept of disaster resilience also has caught on in Oregon, both statewide and locally. For many years, the University of Oregon has developed and delivered an international list for Disaster-Resistant and Disaster-Resilient Universities, in support of FEMA's original mitigation program for colleges and universities. After the original federal funds for the university's program were depleted, it should be noted, the university broadened the program to cover all emergency-management practitioners who directly serve campuses. The University also has established the Oregon Partnership for Disaster Resilience, an applied research center at the University's Community Service Center, that includes a number of continuing blogs on the subject.

On the federal level, the National Academy of Sciences last month conducted a town hall meeting on disaster resilience in – very appropriately – New Orleans, Louisiana; the city and state are still recovering, of course, from Hurricane Katrina and their resilience efforts after that disaster are exemplary and were among the principal topics discussed.

On an international basis, the Asia Pacific Collaborative Security Consortium (APCSC) has developed and is using an innovative Disaster Resilience Visualization and Assessment Tool. The APCSC is a virtual network of five Hawaii-based, Department of Defense-funded, organizations that have a common interest in sharing “enabling” information to enhance and improve regional security and stability. The organizations use the APCSC portal to exchange course-related information with fellows, a practice that is designed to “socialize” future alumni to the practical benefits of continued on-line collaboration after they return to their countries. The even longer-term intent, of course, is for APCSC, or its next-generation replacement, to function as an effective focal point for information-sharing during a future regional crisis and/or as a key information tool supporting collaboration asset available for use on longer-term regional

security projects. The assessment tool presents global information in a user-friendly visual format, allowing users to select their own preferred data layers and areas of interest.

Several nations of Southeast Asia are working on major resilience and recovery programs as a follow-up to the 2004 tsunamis that killed more than 150,000 and caused billions of dollars of damage, some of which is still being discovered. It is not always remembered that not one tsunami but several tsunamis struck and ravaged coastal regions all over the Indian Ocean, devastating numerous nations and entire regions, including: the Indonesian province Aceh; the coast of Sri Lanka; coastal areas of Indian state of Tamil Nadu; the resort island of Phuket, Thailand; and even countries as far away as Somalia – 2,500 miles west of epicenter.

Following are three additional international tidbits demonstrating the still emerging global recognition of resilience:

- (a) The United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) published a discussion paper in 2008 on its Project on Building Community Resilience to Natural Disasters through Partnership.
- (b) After the recent floods in Australia, 68 projects “to boost natural disaster resilience” were announced by the governments of the heavily ravaged Queensland area governments – which see the projects as the foundation for a new regional Natural Disaster Resilience Program.

(c) In South Asia, the government of India is making “Disaster Resilience Audits” mandatory for industry; India is the first nation to do so, according to the Daiji World newspaper and website.

As more time passed and there was a dawning realization that the vast amount of critical infrastructure throughout the United States could not be fully protected 24 hours a day, seven days a week – except by the expenditure of astronomical funding amounts – resilience has come to be recognized as a better practical option that would be more sustainable over the long run as well

Kay C. Goss, CEM, possesses more than 30 years of experience – as a federal and state administrator and in the private sector – in the fields of emergency management, homeland security, and both public finance and intergovernmental operations. A former associate FEMA director in charge of national preparedness training and exercises, she is a noted lecturer as well as the author of several books and numerous articles and reports in the fields of homeland defense and emergency management.

The Lincoln County List of Resilience & Recovery Essentials

Lincoln County, Oregon, acting on the slogan “Creating a Prepared Community,” has developed and distributed both a Disaster Resilience Kit of essential emergency supplies and a practical list of helpful recommendations that individual citizens as well as both public agencies and private-sector organizations, and businesses, will find useful in preparing their own resilience and recovery plans. Included on the Lincoln County list are the following items and suggestions/recommendations:

- An emergency contact list and copies of disaster planning documents;
- An all-hazards NOAA (National Oceanic and Atmospheric Administration) Weather Radio (NWR) and battery-operated or wind-up AM/FM radio;
- Working smoke detectors and a fire extinguisher;
- A First-Aid kit – pre-packed with such essentials as scissors, tweezers, a variety of Band-Aids, gauze pads/roller gauze and tape, anti-bacterial wipes, first-aid ointment, a cold pack, vinyl gloves, a first-aid manual, and various other essential items such as pain relievers and even a small supply of prescription medications;
- One or more flashlights and light sticks;
- Bottled water and nonperishable food (enough to last three days) – plus at least one gallon per person per day in portable-sized containers;
- A variety of nonperishable food, eating utensils, and at least one can-opener;
- A reasonable number of essential office and “household” supplies – including pens, pencils, pads of paper, duct tape, markers, toilet paper, tissues, paper plates, napkins, and both face cloths and towels;
- Various “handyman” tools and supplies – including duct tape (again), waterproof plastic sheets, a shut-off wrench (for water and gas), a whistle, at least one plastic bucket (with a tight lid), work gloves, pliers, a hammer, plastic garbage bags, zip-ties, rope, and wire;
- Also: a pry bar, a shovel, dust masks, eye protection, all-weather gear, and both a push broom and a mop;
- Camera – either a disposable camera or one with extra batteries and the film needed for recording damage;
- Cash – enough “folding money” as well as the cash and change needed both for immediate needs and to serve customers if ATMs and credit/debit machines are not working (most of the cash should be in smaller denominations);
- Manual credit-card backup – a manual credit card machine is needed as a back-up if/when the power is out; and, last but not least;
- One or more cell phones – plus an extra charger (not only at home but also at work).

The Three “T”s of Terrorism – Finding the Facts in the News

By Jordan Nelms, Viewpoint



The early minutes, hours, and days following a terrorist attack or similar incident – e.g., the 24 January 2011 Moscow bombing at Domodedovo Airport, or Jared Loughner’s 8 January 2011

Tucson shooting spree – were, in only a few short minutes, filled with speculation and a broad spectrum of assumptions, many of them totally unprovable, about the perpetrators of the attack and their *modus operandi*. Such uncertainty and unverified rumors are similar in many ways to what is called the fog of war, and might accurately be described as the fog of crisis.

In the 24-hour news cycle, there is a constant stream of information being generated from a broad spectrum of “sources,” some of them well informed, but others not. With so many interpretations being offered, it is important that not only homeland-security professionals but the general public as well be able to carry out their own fact-check assessments of a major mass-casualty event or incident, relying on those facts rather than on amateur speculations and unwarranted assumptions.

When analyzing a terrorist attack – failed or successful – there are in most cases at least a few fundamental and verifiable facts worth considering. Despite the limited amount of information usually released by official government spokesmen during and immediately after the initial phase of an investigation, outside observers can use at least some seemingly reliable media reports and open intelligence sources, and/or even surf the internet, to develop a few reasonably informed conclusions of their own – which in most cases should be based on what might be called “The Three ‘T’*s*” of a terrorist attack – *Target*, *Tactics*, and *Technology*.

Clear Thinking and an Open Mind

Here, a word of caution is necessary: Far too often, political pundits and news anchors – using unquoted and unnamed sources – are quick to conclude that one well known group

or another, usually one already in the news, has perpetrated a specific attack. Knowing what information to focus on in these news reports, and how to apply that information to think somewhat more critically – more logically, in other words – about the event, is an important skill for any media consumer, particularly in the face of sudden disaster. Keeping that point in mind, it is usually possible, focusing on the Three T’s, to develop at least a few tentative conclusions, as follows, from the limited evidence that is available:

1. **TARGET** – Knowing with reasonable certitude what person, group, or organization was the probable target of the attack will usually (but, of course, not always) permit the development of some reasonable assumptions about the terrorist organization responsible for the attack. By definition, most terrorist groups have publicly stated the political objectives for which they are fighting. The target of an attack by a specific group, therefore, can frequently be determined by analyzing the group’s known political goals and objectives. Determining the group’s most likely targets – which might range from indiscriminate civilian population centers to political institutions – can provide valuable information about the possible motives of the individual or organization launching an attack. Political institutions, public transit systems, and places of religious worship all represent what many terrorist groups might well consider to be “ideal targets” for getting an ideological message to an intended audience.

There are significant differences in that message, of course, when the target selected is the civilian population, a symbol of authority (a police station or other government building, for example), critical infrastructure such as a power plant, or individual political officials. Through fear and coercion, even a failed attempt to attack a well known target can have dramatic consequences, primarily because it sends such a clear message – namely, that an attack is possible, even in

In the 24-hour news cycle, it is important that not only homeland-security professionals but the general public as well be able to carry out their own fact-check assessments of a major mass-casualty event or incident, relying on those facts rather than on amateur speculations and unwarranted assumptions

the middle of a suburban shopping center or against a major transportation center such as an airport or subway system, both of which are today heavily guarded, or at least monitored, by law-enforcement agencies.

2. TACTICS – In the initial moments following a terrorist incident, knowing the terrorists’ tactic of choice, which is usually quite obvious, can be useful in assessing the capabilities of the perpetrator. It is not always necessary for terrorists to launch major attacks such as al Qaeda’s destruction of the World Trade Center towers on 11 September 2001 to achieve their goals. In the business of fear and intimidation, striking targets that are both unprotected and unprepared is of considerable value to the terrorist organization. In fact, the methods of attack have in recent years, and for various reasons, moved toward the use of a lone gunman rather than a group of suicidal extremists. Nonetheless, the continued use of suicide bombers and of improvised explosive devices (IEDs) is proof in itself that these methods still work and are likely to be continued far into the future. However, a single terrorist in a shooting-spree scenario typically (but not always) represents only a lone gunman acting on his/her own accord.

Conversely, the ability to destroy a selected target by using an IED – then getting away to fight another day – gives the individual terrorist the ability to make numerous attacks with minimal financial resources. In fact, publicly available do-it-yourself IED manuals can easily be obtained over the internet. Moreover, the IEDs themselves can be assembled by persons possessing little or no in-depth knowledge of chemistry or explosives. The complexity of the IED itself, therefore, can be a helpful clue to the level of training the terrorist group or individual terrorist probably has received. The use of a suicide bomber – a tactic seen most frequently, but not exclusively, in the Middle East – typically points to an organization with deep roots in Islamic Extremism, which sees the taking of one’s own life for a religious cause as a form of martyrdom.

3. TECHNOLOGY – The level of technology used in a terrorist attack often provides the foundation for a more thoughtful assessment of the particular terrorist organization that might be involved. A comparative analysis of the technology used in attacks of similar scope will probably show at least some similarities and/or differences in the resources available to a terrorist organization. Comparing the technology of last month’s Domodedovo attack – in which the terrorists used 5-10 kg of trinitrotoluene (TNT) stuffed with metal objects, includ-

ing screws and metal balls, according to open-source intelligence reports – to al Qaeda’s failed 2009 Christmas Day attempt, using pentaerythritol tetranitrate (PETN – a very powerful high explosive) to blow up an airplane en route to Detroit provides a clear indication of the various resources available to totally different organizations striking similar aviation targets.

Larger terrorist organizations usually have more resources they can draw on for “best practices” in building explosive devices that can maximize casualties. Many but not all of the IEDs used in attacks in Iraq and Afghanistan, in fact, have used various chemical combinations, usually concealed in hidden devices packed with ball bearings, nails, and other shrapnel-like materials to increase not only the number of deaths but also the property damage resulting from the explosion. The presence, or absence, of these explosive components can be and frequently is a reliable indicator of the possible source of the device schematics and often provides other credible clues about the origin of the terrorist.

Without the forensic and investigatory resources needed to run fingerprints and review closed-circuit television footage, media consumers often are provided only the usually limited information that public officials are willing and/or able to make public. Nonetheless, the three essential elements, described above, of most terrorist attacks provide the basic framework needed for thinking more critically about the facts available and will allow everyday citizens to question the conclusions that are being offered by the news media and/or by public officials charged with investigating such attacks. In short, by focusing on the Target, Tactics, and Technology aspects of a specific incident, the average media consumer can be empowered to draw his or her own conclusions – and quite possibly come much closer to “the real truth” than is possible by simply accepting the information provided, even with the best of intentions, by the media and/or the public officials investigating the attack.

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).

USCG's Small-Vessel Security Strategy Ready for Launch

By Corey D. Ranslem, Coast Guard



Attacks by small vessels around the world are increasing in intensity against both larger vessels and shore-side facilities. In addition, piracy against vessels of all types is spreading to different parts of the world. Pirates currently hold over 30 vessels and 700 mariners. Over the past weekend, pirates hijacked a U.S.-flagged sailing vessel and killed the four Americans onboard. Pirates successfully use small vessels to carry out their attacks. Islamist extremists have used small vessels in many attacks in the not-too-distant past, including the attack in Yemen on the USS Cole and, more recently, in the terrorist plan to go ashore and wreak havoc in downtown Mumbai, the largest city in India.

These types of attacks and others highlight the general vulnerability – throughout the world – of ports, cargo vessels, cruise lines, and coastal facilities. Moreover, such threats continue to increase worldwide. An attack by a small vessel on a port, vessel, or coastal facility will have a negative worldwide economic impact. Further complicating the situation is that detection of small-vessel threats in many regions is very difficult because attackers use vessels that would normally be seen in the particular area or region being attacked. Pirates use local fishing vessels, in fact, to carry out many of their attacks, and larger vessels have trouble identifying which fishing vessels are legitimate.

The same would be true, of course, of an attack in a U.S. port and/or in the nation's coastal waters, where the attackers would probably use yachts or other pleasure vessels to carry out their attacks, making it extremely difficult for law-enforcement agencies to identify them. The U.S. Coast Guard and its parent agency, the Department of Homeland Security (DHS) have worked with various stakeholder groups throughout the United States to understand and develop an effective strategy to counter the potential small-vessel security threat to the nation's ports and waterways.

Completed, But Not Yet Approved or Promulgated

That strategy has recently been finalized, in draft form, and is now awaiting formal approval from DHS and the White House. It seems likely, though, that the classified and unclassified versions of the final document should be out within the next few months. Meanwhile, Coast Guard officials have been working with various stakeholder groups across the country to develop implementation plans and policies. Much of the input has come from state and local law-enforcement agencies, recreational boating organizations, and other marine and maritime groups and associations, both public and private.

Pirates use local fishing vessels, in fact, to carry out many of their attacks, and larger vessels have trouble identifying which fishing vessels are legitimate; the same would be true, of course, of an attack in a U.S. port - where the attackers would likely use yachts or other pleasure vessels to carry out their attacks, making it extremely difficult for law-enforcement agencies to identify them

Congress, DHS, OIG (Office of Inspector General), and other federal agencies have identified the small-vessel security threat as one of the greatest dangers facing the U.S. maritime industry and the nation as a whole. Many experts believe, in fact, that a small-vessel attack similar to the one against the USS Cole could easily be carried out in a number of U.S. ports against cargo vessels or even cruise ships. Making the security task immensely more difficult is the fact that the perennially undermanned U.S. Coast Guard has approximately 95,000 miles of coastline and inland waterways to protect, and numerous other responsibilities, so obviously cannot handle the job alone.

Nonetheless, over the past four years the Coast Guard has been meeting with various stakeholder groups – ranging from local law-enforcement agencies to pleasure boating groups to shipping companies – to develop a collaborative strategy to deal with the small-vessel threat. “We have conducted hundreds of meetings and briefings on the subject of the small-vessel threat and how we can mitigate that threat with various stakeholders,” comments Robert Gauvin (Executive Director of Piracy Policy, Technical Advisor, Office of Vessel Activities, at Coast Guard

+ Disaster Response and Recovery EXPO



MAY 3-4, 2011 • GAYLORD TEXAN HOTEL AND CONVENTION CENTER • GRAPEVINE, TEXAS

“DRRE 2010 and for that matter all previous DRRE conferences have been our company’s single best conference to reach the largest majority of Mass Decon Teams in the US that is held today! We at CON-SPACE will continue to attend this valuable show for 2011 and well beyond!”

—Bill Johnson,
National Sales Manager,
CON-SPACE

“The Disaster Response & Recovery Expo has always been a great show for CommandAware. DRRE allows us to interact with our target audience, network with other organizations and build strategic relationships with other vendors.”

—Heather Sabo
National Client Relations
Manager
CommandAware |
Concerro, Inc.

Discover the Latest Disaster Response & Recovery Equipment, Technology and Services!

Co-located with the Integrated Medical, Public Health, Preparedness and Response Training Summit (ITS), the Disaster Response and Recovery Expo (DRRE) is the perfect opportunity to discover the latest in:

- Crisis Communications
- Computer Software/Hardware
- Decontamination Shelters & Equipment
- Emergency Lighting
- Healthcare Systems
- Information Technology
- Hazmat Response Equipment
- Mass Casualty Systems
- Mobile Response
- Medical Surge Supplies and Equipment
- Pharmaceuticals
- Power Sources
- Public Health & Safety
- Public Works
- Safety and Rescue Equipment
- Shelters
- Social Services
- Vehicles
- Water Systems
- And More!

Exhibit at DRRE and Tap into the \$60 Billion Emergency Response Market! Contact:

DRRE Exposition Management
c/o J. Spargo & Associates, Inc.
800-564-4220 / 703-631-6200
drre@jspargo.com

DRRE is sponsored by the Chesapeake Health Education Program, Inc.



For more information and to register visit www.drreexpo.com

Headquarters). “The stakeholders are an important part of the small-vessel security strategy because they possess local knowledge and will know and see what does not seem to fit.”

Gauvin has been the Coast Guard’s lead in developing the new strategy and in working with the key stakeholder groups. “We held a stakeholder summit in Washington, D.C., to bring as many of the stakeholders together as possible to identify a strategy that will not put undue economic stress on the recreational boating public,” says Gauvin. “We walked away from the first summit in 2007 feeling good about moving forward. We had over 78 percent participation in the post-conference survey, which gave us a good idea of the stakeholders’ viewpoint.”

The Global Impact of a Successful Attack in U.S. Waters

It is currently estimated that there are over 26,000 small vessels (under 26 feet) registered throughout the United States. Moreover, the nation’s marine industry has an estimated \$742 billion economic share of the overall U.S. economy. For that reason alone, if there were a small-vessel attack “on a port within the United States,” Gauvin commented, “the negative economic impact of that attack ... would be felt worldwide.

“Sometimes people do not realize,” he continued, “the importance of the [U.S.] commercial and recreational marine industry and its economic impact worldwide.” Close to 99 percent of the world’s cargo is moved aboard commercial ships, and many U.S. ports are located within major metropolitan areas. Moreover, most of the direct law-enforcement and emergency-response operations within U.S. ports are handled by local law-enforcement departments, fire and rescue agencies, and private-security companies.

“Developing the final strategy has been a hand-in-hand partnership with local, state, and federal response agencies and the recreational boating public,” says Gauvin. “Agencies across the board have been working together, better than ever before, in developing the new strategy.”

Officials said that the DHS leadership will continue to work with local, state, and other federal agencies, along with the recreational boating industry, to implement the final strategy after it has been approved by DHS and the White House. Gauvin said he believes that the final strategy will probably be released sometime this spring.

Corey D. Ranslem, chief executive officer of Secure Waters LLC – a maritime-security and consulting firm heavily involved in maritime training, maritime security, and a broad spectrum of other programs in the maritime field -- is the former regional manager of Federal Government Operations for Smiths Detection. He has received numerous awards and citations from the U.S. Coast Guard and other agencies and organizations active in the field of maritime security.

Special Event Planning Survey

Your Opinion Matters!

Each year, thousands of entities – including government agencies, private volunteer organizations, and commercial enterprises at all levels – engage to plan and oversee a wide array of special event activities across the country. These events vary greatly in terms of size, scope, and complexity.

DomPrep wants to know **your opinion** on the application of special events-focused security and emergency best practices, planning structures, and information-sharing mechanisms to broaden community preparedness in an all-hazards context.



Take
Survey

Storm Warnings: Communications and Utility Resilience

By Omar Alkhalaf, Viewpoint

In the field of emergency management, resilience is directly correlated to preparedness. Proper planning, combined with the execution of emergency plans prepared for weather-related emergencies, can significantly improve the outcome of such emergencies. In addition, the establishment of proper communication channels helps ensure that services are restored in a timely fashion.

The 2007 winter storms in Iowa and the 2008 ice storms in New England are among the more prominent examples in recent years that highlight the need for effective communications plans to ensure that power utilities are resilient both during and after weather-related emergencies. These events, and the thorough after-action reviews that followed, provide important lessons for other jurisdictions.

During the winter of 2007, the state of Iowa experienced two historic storms that knocked out power to an estimated 134,000 or more of the state's residents. The loss of power also affected the telephone systems that were dependent on power and ultimately prevented many constituents from reaching emergency services. Improved communications between utility companies and the state, it was obvious, would allow government officials to have a more accurate, and more timely, understanding of the areas in need of immediate assistance – and also, in 2007, would have enabled the re-direction of the telephone lines dependent on power to ensure access to emergency services.

One of the more important lessons learned from this incident focused on the activation of emergency plans to ensure that proper resources are allocated to address both the loss of power and the impact that a lack of those resources has on the state's critical infrastructure.

N.H.: A Helping Hand From Neighboring States

In 2008, New Hampshire experienced a major ice storm that caused over 400,000 customers to lose power, an impact felt by all four of the state's major utility providers. The magni-

tude of the storm caused the providers' infrastructure to suffer considerable damage – enough, in fact, that they were forced to request help from providers in neighboring states.

In this case, New Hampshire had developed emergency “what if” plans with neighboring states in advance of what turned out to be a worst-case situation. The lack of communications, and of standardized methods of response, however, adversely affected the ability of utility companies to respond to the outages. The after-action report issued following a review of the 2008 incident highlights the need to institute trigger points in the system that would automatically mobilize resources to ensure a more timely restoration of services. The report also recommended that utilities conduct readiness drills that would include participation by all relevant support organizations.

The 2007 and 2008 storms provided numerous lessons to the utility industries of both New Hampshire and Iowa, and served as both a warning and an example for other states. The ability to have a clearly defined and well rehearsed response will usually allow the restoration of utilities in a quick and organized fashion, thus minimizing the risks associated with damages caused to such critical systems. Without adequate communications, however, the restoration of power utilities could suffer greatly. By ensuring that stronger and more reliable communication channels are available, and

that appropriate operating procedures are in place, future emergencies of similar magnitude will be addressed not only more promptly but more effectively as well.

For additional information on similar incidents and detailed after-action reports, please visit the Lessons Learned Information Sharing Web site at www.llis.dhs.gov.

Omar Alkhalaf is an outreach and operations analyst for Lessons Learned Information Sharing (LLIS.gov), the U.S. Department of Homeland Security/Federal Emergency Management Agency's national online network of lessons learned, best practices, and innovative ideas for the nation's homeland security and emergency management communities. He received a bachelor's degree in Global Affairs with dual concentrations in Global Diplomacy and Governance/Middle East & North Africa Region from George Mason University in Northern Virginia.

Air National Guard Resumes Life-Saving CCATT Mission

By Ellen Krenke, National Guard



After a six-year hiatus, the Air National Guard is back in the Critical Care Air Transport Team (CCATT) business.

“As the Guard migrated into the homeland defense mission, we got away from the CCATT mission,” Air Force Colonel Brett Wyrick – air surgeon for the Air National Guard – told participants in a Department of Defense “Live Bloggers Roundtable” on 11 January 2011. “However, recently what we discovered is that there is a need for the Air National Guard in the CCATT mission, and also we ... [have] quite a bit of expertise in the Guard and in the Reserve that allows us to meet the demands of the mission and take some of the strain off the active-duty ... [forces] who have been stretched quite thin by the ongoing conflicts.”

The CCATT concept was introduced by the Air Force surgeon general about 10 years ago to meet a need for transporting the most critically injured patients by using the aeromedical evacuation system. “This is a mission where we actually bring ... everything that you would find in an intensive care unit to the air frame,” Wyrick said. “And it gives us the ability to move injured and wounded Soldiers and Airmen, Marines ... from the forward areas of the battlefield back to a tertiary-care facility either in Europe, the Pacific, or the [continental] United States.”

A CCATT consists of an intensive care physician, a critical care nurse, and a respiratory technician. The first Air Guard CCATT team is currently on alert at Ramstein Air Force Base in Germany. If there is a need “downrange,” Wyrick said, the team “can deploy forward from Ramstein into Iraq, Afghanistan – or even into the African continent, if there’s a need for that, and then they ... [are transported with] the patients back to the United States or back to Europe, wherever the mission [dictates].”

Eighteen CCATTs & a “Constant and Persistent Line”

After the CCATT mission requirement was validated, it took less than six months for the Air Guard to field its first team – with the help of the Air Force Expeditionary Medical Skills Institute’s Center for Sustainment of Trauma and Readiness Skills at the University of Cincinnati.

“We’re going to have a constant and persistent line in the AEF now ... [and] for the next two years out of Ramstein,” Wyrick said. The Air Guard plans to stand up 18 full CCATTs from 17 states, he added. Many of them have already started training, and are expected to reach full operational capability within the next two years.

The Air Guard also has volunteers from all 54 U.S. states and territories who would be available to augment the teams if and when needed. “There’s a number of Guardsmen out there from various states who want to participate in the mission, who have the medical training and qualification to participate in the mission,” Wyrick commented, “and we’re ... accepting them as volunteers.” The members of the team at Ramstein are Colonel Bruce Guerdan, the state air surgeon for the Florida Air Guard, Lieutenant Colonel David Worley, a nurse from the Kentucky Air Guard, and Master Sergeant Jody Nitz, a respiratory therapist from the Michigan Air Guard. “So, we did combine ... people from all over the country to put these volunteer teams together,” Wyrick pointed out.

The doctors on the team will rotate every 30 days or so, and the nurses and respiratory technicians will average about 60 days – but at least one nurse has volunteered to do six months. All of these Air Guard medical personnel have one major asset in common – experience. According to Wyrick, the average Guard physician has at least 15 to 20 years in medicine, much of that time in primary care; most also have an active-duty background. After leaving the military, the team members typically upgrade their skills by either re-specializing or sub-specializing.

A Multi-Talented Total Force Partner

The full CCATT roster includes “a lot of critical care physicians, a lot of surgeons, anesthesiologists,” Wyrick continued. “Guys who have literally written the book on modern medicine are residing in the Air Guard. And by putting them in the CCATT mission, we bring years of experience and ... years of knowledge that make us a good Total Force partner for the Air Force.” Many of the volunteers already have CCATT experience, while others bring their experience as specialists in the civilian health care world and therefore are readily trainable for the CCATT mission.

In addition to carrying out its federal mission, a CCATT could also be used for emergency responses in the United States itself. “If we had a situation on the Gulf Coast where a big hurricane rolls up on shore and you need to evacuate civilian patients from a civilian hospital in the hurricane’s path,” Wyrick pointed out, “that would be another use for the CCATT teams.” Reactivation of the CCATTs “gives you a way to transport ... critically injured patients from the strike zone to areas of safety,” he said. “So it’s not just battlefield and combat casualties; it could also be in humanitarian roles or in a disaster situation.”

Individual states now have access to Air Force equipment in the event of a disaster, because many previous barriers no longer exist. In the wake of Hurricane Katrina, Wyrick noted, there was “a lot of crosstalk,” followed by “a lot of planning, and we [now] have access to the equipment and supplies that we need when we need them.”

Among the equipment used by the Air Guard CCATTs are life-support systems and devices that have been tested and verified as being both safe and airworthy. “When you are talking about transporting patients through the air, you know,” Wyrick commented, “what you have is what you bring with you. And those systems have to be super-reliable, there [must] be redundancies in there, and they have to be safe ... for flight.”

Fully Equipped, Ready to Fly & Always Alert

The typical CCATT patient will arrive “fully equipped,” so to speak, with a stretcher, a monitor, and intravenous pumps, as well as a ventilator (to maintain the patient’s respiration throughout the course of the mission). In addition to the equipment, the CCATTs fly with a full aeromedical evacuation crew, most members of which are providing care for the less critical patients also being transported. However, depending on whether the mission has been previously scheduled or is a last-minute assignment, the CCATT may not always have an aeromed crew along on every flight.

“In a pinch, these guys can convert anything into ... [an] airevac platform,” Wyrick commented. He said that the Air Force has shifted away from the original aeromedical evacuation mission concept insofar as the specific air frame required. CCATTs are the “back-end medical crew. As far as the aircraft goes, the CCATT teams can use an aircraft of opportunity and, while everybody prefers to have a C-17 [Globemaster transport aircraft] – because of the design and the room ... we also fly missions from the theater far forward in Afghanistan back to the United

States in KC-135s [aerial refueling aircraft], or we can also ... [use] a C-5 [Galaxy transport aircraft] or whatever aircraft is designated as the aeromedical evacuation platform.”

Only the most critical patients will require use of a CCATT team. “What we’re doing,” Wyrick explained, “is we’re taking patients that otherwise wouldn’t be candidates for the aeromedical evacuation system because ... we really are talking about the most severely injured patients there [at Landstuhl, Germany, headquarters of a U.S. Army regional medical center].”

Each CCATT can handle up to four patients – who usually are flown directly from Landstuhl back to Andrews Air Force base just outside of Washington, D.C., and from there they are taken by ambulance to the Walter Reed Army Medical Center in D.C. or to the National Naval Medical Center a few miles away in Bethesda, Maryland; some patients, though, will be taken directly to the burn center at the Brooke Army Medical Center in San Antonio. How quickly a patient is transported back to the United States usually depends on the needs of the individual patient.

Wyrick notes that patients from the forward areas often require additional surgery. “After they’ve undergone the combat resuscitation and stabilization, then when they get to Landstuhl, there could be ... other procedures that are done where they take the patient back to the [operating room] ... and then it might be several days or even weeks before the patient is actually ready for transport back to the United States.” A patient who has suffered a serious burn, though, he added, would usually be transported almost immediately to San Antonio.

The first of the reactivated Air Guard CCATTs was scheduled for its first flight back to Andrews on 11 January 2011, but there were no critical-care patients waiting for transport from Landstuhl back to the United States. “That’s actually ... a good thing,” Wyrick commented. “Because the fewer injured patients there are for the United States military, the better things are going. So they’re sitting alert right now, and they’re ready.”

Air Force Lieutenant Colonel Ellen Krenke is a public affairs officer currently assigned to the National Guard Bureau’s Office of Public Affairs and Strategic Communication. She has held many positions at the bureau, including duty as chief of command information. Krenke also has served as a desk officer for the Office of the Secretary of Defense-Public Affairs. Before joining the Air Force she was a sportswriter for the Arkansas Democrat-Gazette in Little Rock. Krenke has received numerous awards from Arkansas press associations for her in-depth reporting, investigative reporting, and sports feature writing. She also has been selected as the NGB’s Journalist of the Year.

Georgia, California, Kansas, and Colorado

By Adam McLaughlin, State Homeland News



Georgia **Marietta Upgrades Wireless Net to Improve Responder Coordination**

For policemen and firefighters in Marietta, Georgia, the 2009 upgrading of the city's wireless network to Third Generation (3G) communication networks and devices has not only given them faster and better access to information – as well as more time spent outside the station – but also has improved their resource tracking capabilities as well.

But that was only the beginning, as it turned out. Late last month the city started working with its vendor to test an upgraded 4G version. “That is probably the biggest development going on right now,” said Ronald Barrett, the city's management information systems and GIS (geographic information system) director. Approximately 70 percent of the city is currently covered by Sprint's 4G service, he added.

Marietta had been using 19.2 Kbps modems, installed in the city's police and fire department vehicles, since the late 1990s, and those units and other equipment were beginning to wear out and needed replacement. Moreover, the older modems had cost \$2,200 each, and city officials determined that they could not only save money and provide more and better applications but also cut expenses by using new and faster modems that cost only \$795 each.

Marietta purchased Utility wireless routers to upgrade its overall mobile communications capabilities. Deployment of the new routers started with the city's police vehicles, then expanded to the fire department and other city agencies.

The greater bandwidth now available provides opportunities for more applications and greater management flexibility in general. The city's Information Technology (IT) department is developing a crisis-management system that will: (a) accept updates from officers and firefighters in the field; and (b) communicate updates from the command center back to personnel in the field. “They [the responders] can be out in the field and they do not have to call something in and say, ‘OK, I picked this guy up here,’” Barrett commented. Instead, he added, the responders simply “mark it on a map so they can keep up with an event with multiple incidents involved.”

An automatic vehicle location system is built into the modems, which are equipped with, among other improvements, new “charge guards” that will keep the modems powered for up to four hours after the vehicle is turned off. In addition, the GPS (global positioning system) antennas built into the new modems not only are harder to tamper with but also allow vehicles to be tracked more accurately – and without exposing an antenna on the roof of the vehicle.

The upgrades also keep officers from having to physically go back to the station as often. New capabilities allow officers to send a document to a printer in the station directly from their police cars and ease the overall troubleshooting workload for the entire IT staff. “As long as they have a connection,” Barrett said, “we can remote into their desktop and administer it just like it is a laptop or a personal computer on the Local Area Network; probably 70 percent to 80 percent of the problems now we can fix remotely.”

California **San Diego Completes Major Water Pipeline Project**

In late January the San Diego County Water Authority completed the new San Vicente Pipeline, which will provide the entire region with fresh water in the event of a major earthquake, drought, or other disruption.

San Diego currently receives 90 percent of its water from two distant sources, making it susceptible to disruption in the event of a major disaster. Snow melt from the Rocky Mountains feeds the Colorado River, which in turn supplies water to Lake Havasu – which is where the San Diego County Water Authority has built a 242-mile-long aqueduct to provide water to meet the needs of the county's more than three million residents.

A 444-mile-long aqueduct stretching from Northern California is the county's other primary source of water. The Sacramento-San Joaquin Delta provides the water for the aqueduct with snow melt from the Sierra Nevada Mountains.

The San Vicente Pipeline, an 11-mile, 8.5-foot-diameter pipe, was funded as part of a \$1.5 billion Emergency Storage Project that was initiated to ensure that the San Diego region would

have access to fresh water in the event of a major disaster that interrupted the flow from the Sacramento-San Joaquin Delta. The new pipeline, which begins in Lakeside and ends in Mira Mesa, will provide water to residents of the southern half of the county.

The county also is expanding the capacity of the San Vicente dam, raising it an additional 117 feet so that its walls will soon reach a height of almost 340 feet. The expansion project was initiated two years ago and is expected to be completed by early 2013. When finished, the reservoir will hold an additional 152,000 acre-feet of water and annually provide roughly 300,000 homes with the fresh water they need.

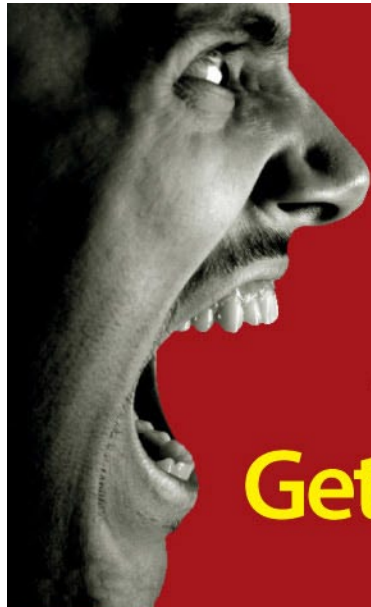
With San Diego's primary sources of water drying up, local water projects such as the San Vicente Pipeline will become increasingly important. San Diego residents depend on melting snow from the distant Rocky Mountains and the much closer Sierra Nevada Mountains to provide them with water – but even the most optimistic climate models show that anywhere from 30 percent to 70 percent of the snow pack may well disappear in the second half of this century. “There is a two-thirds chance there will be a disaster,” said Nobel laureate Steven Chu, secretary of the U.S. Department of Energy, “and that’s in the best-case scenario.”

Kansas DHS Funds Sought for National Bio And Agro-Defense Facility

A \$150 million allocation within President Barack Obama's 2012 budget plan is good news for the federal biosecurity lab slated for construction in Manhattan, Kansas. If approved by Congress, the money will keep construction on track for the \$650 million National Bio and Agro-Defense Facility (NBAF), scheduled to open in 2018. The allocation for the Department

of Homeland Security (DHS) was one of many major construction projects included in the \$3.7 trillion budget plan Obama sent to Congress on Monday, 14 February.


“Clearly, this is encouraging news to see this [allocation] high on the president's priority list,” said Ronald Trewyn, vice president of research for Kansas State University (KSU). “To strengthen our resilience by developing the capability to produce vaccines and therapeutics rapidly



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

and inexpensively, the ... DHS and the U.S. Department of Agriculture [USDA] have the joint responsibility to protect our nation's animal agriculture and public health from these threats. The Department is leading these efforts through the construction of the NBAF in Manhattan."

The announcement comes, though, at a time when a previously requested \$40 million in NBAF funding for 2011 is still uncertain. Congress has not yet passed a final fiscal year 2011 appropriations bill, but the NBAF funding previously requested is included in a comprehensive "continuing resolution" bill scheduled to be reviewed in March.

In the past, both Obama and his predecessor, President George W. Bush, have specifically allocated money for the NBAF project. But the \$150 million requested for the next fiscal year, which starts on 1 October 2011, is by far the largest amount ever designated for the facility and marks a major increase in the funding needed to complete the project.

"This is a big step forward," said Kansas Bioscience Authority President and CEO Thomas Thornton. If the funding requested for fiscal year 2012 is approved by Congress, he noted, the money provided would be used for actual construction of the lab itself. The groundwork is already being laid for that step of the project; roads and utilities are now being rerouted on the 45-acre site (across the street from the KSU football stadium), and design plans for the building are 35 percent completed.

Meanwhile, the university is also boosting its research, with the help of funding provided by the Kansas Bioscience Authority, on many of the same deadly animal diseases that will soon be studied at the NBAF labs. In addition, construction of the central utility plan is scheduled to begin this summer. The building of the lab itself probably will take several years, but should be finished by 2017. The NBAF is expected to be operational by 2018.

Colorado Education Department Focuses On School Emergency Communications

The Colorado Department of Education (CDE) has announced that a \$41.5 million fund tied to the National School Lunch Act may be used to pay for some upgraded emergency communications systems needed at schools throughout the state.

The 4 February announcement, at the Colorado State Capitol in Denver, was a highlight of a "School Safety Summit" – which was formed under the leadership of Theodore Hughes, director of the CDE's division of capital construction assistance, and included a group of 25 school-safety stakeholders who decided on legislative proposals and reviewed both funding opportunities and training resources.

Hughes said that his office's Qualified Zone Academy Bond (QZAB) program could be used to finance technology that would improve communications between schools and first responders during an emergency. The schools in more than two thirds of Colorado's school districts, according to Hughes, would qualify for QZAB funding – which can be used for, among other things: providing equipment; training teachers and other school personnel; rehabilitating or repairing school facilities; and/or developing course materials.

The QZAB funds are available to schools in which at least 35 percent of the students are eligible, under the National School Lunch Act, for free or reduced-cost lunches. CDE figures show that over 252,000 K-12 students, an estimated 39 percent of all of the K-12 students in the state, are eligible for the lunch program. State senator Steve King, who led the summit, said he expects to introduce the legislation needed to establish the new communications plan on 18 February.

The purpose of the state's strategy is to adhere to guidelines included in the National Emergency Communications Plan (NECP), created by the U.S. Department of Homeland Security (DHS). Those guidelines are designed to promote the ability of emergency-response providers, and government decision-makers: (a) to continue to communicate in the event of natural disasters, as well as acts of terrorism and/or other manmade disasters; and (b) to ensure, accelerate, and attain interoperable emergency communications nationwide.

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.



the **single solution** for all your needs



irms360
Enterprise

- ASSET Management
- EMERGENCY Management
- MOBILE LOGISTICS Management
- PATIENT Management
- VACCINE Management
- INVENTORY Management
- PROVIDER Management
- HOSTING Services

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 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.

upp.com