

Critical Infrastructure Protection, Resilience, or Both?



A Preparedness Challenge

Transitioning Resilience From Theory to Reality

By Dennis R. Schrader, CIP-R

Has Resilience Become the New Protection?

By Leslie-Anne Levy &
Monica Giovachino, CIP-R

GPS-Equipped Vehicles And the EMS Infrastructure

By Joseph Cahill, EMS

No Easy Choices In Coping With a Nuclear Gorilla

By Neil C. Livingstone, Viewpoint

DomPrep Survey

Your Thoughts Compared with DomPrep40's National Experts on... The Security of National Infrastructure

By John F. Morton, DP40

The Principles of Infrastructure Resilience

By Scott Jackson, CIP-R

Lessons Learned For Critical Infrastructure

By Andrew Pearsons, CIP-R

Pennsylvania, Kansas, California, and Kentucky

By Adam McLaughlin, State Homeland News

Special Report Series: Haiti

Port Recovery in Haiti: The Initial Stages

By Corey Ranslem, Coast Guard

Local Security:

The Forgotten Factor in Relief Operations

By Joseph Trindal, Law Enforcement

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 to reliably protect those you serve.

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

Editor's Notes

By James D. Hessman, Editor in Chief



There was no mention of the word “resilience” in the initial *National Strategy for Homeland Security* – as Leslie-Anne Levy and Monica Giovachino astutely point out in their jointly bylined article in this month’s issue of *DPJ*. The reason was obvious: that first National Strategy was issued less than one year after the 11 September 2001 terrorist attacks – a time when the federal government, and the American people, were much more concerned about the prevention of, response to, and/or recovery from additional such attacks.

But the need for resilience, which is now a popular and absolutely appropriate buzzword, and might loosely be defined as a city’s, or community’s, infrastructure to absorb, mitigate the effects of, and/or quickly recover from almost any type of disaster, natural or manmade, is now much more evident than it was eight years ago. Scholarly papers, books, and special reports have been written about resilience. Several public and private-sector organizations – e.g., the National Infrastructure Advisory Council and The Infrastructure Security Partnership – focus on resilience as one of their key areas of interest. And several divisions and directorates of the U.S. Department of Homeland Security specialize in enhancing and upgrading the resilience of the nation’s critical infrastructure in all states and regions of the country.

In two major related articles in this issue: (a) Scott Jackson discusses the basic principles of resilience – capacity, flexibility, tolerance, and cohesion – and how they relate to “the architecture of an infrastructure”; and (b) Dennis Schrader explains not only how, but also why, resilience has escalated in importance from a little-noticed policy afterthought to a major national priority.

The urgent need for the new focus on resilience is spelled out, in illuminating detail, in a Special Report, by John Morton, on the results of two DomPrep surveys – one reflecting the views of the DomPrep40 group of career professionals and senior decision makers in the field of homeland security; the other comparing those views with the somewhat more diverse opinions of DPJ readers. You are strongly encouraged to read Morton’s report in its entirety – and to personally participate in similar surveys in the future.

Also included in this month’s printable issue are: (a) A chilling analysis, by Dr. Neil Livingstone, on the escalating threat posed by a nuclear-armed Iran not only to Israel and the United States but also to the peace of the entire world; (b) Two timely reports – by Corey Ranslem and Joseph Trindal, respectively, on how the U.S. private sector responded, both quickly and effectively, to the Haitian earthquake – and on the lack of local security that made relief operations much more dangerous than they should have been; (c) An instructive “Lessons Learned” article, by Andrew Pearsons, on the need to make the protection of first responders themselves the first priority in coping with disasters, particularly those involving radioactive or other harmful materials; and (d) A well-reasoned article by Joseph Cahill on the growing capabilities – and, therefore, growing importance – of the EMS (emergency medical services) fleets of “mini-ER” ambulances and other vehicles.

Rounding out the issue are four “States of Preparedness” news updates, by Adam McLaughlin, on significant events and occurrences in the great states of California, Kansas, Kentucky, and Pennsylvania.

About the Cover: Collage, by Susan Collins, of a minuscule fraction of the hundreds of vulnerable U.S. and allied infrastructure components that could be attacked – massively, and without warning – by international terrorists. (iStockPhotos show a Paris Metro stop; O’Hare Airport in Chicago; a truck being unloaded in Anywhere, USA; the Manhattan skyline; and a cargo ship docked in Baltimore.)

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
scolins@domprep.com

Catherine Feinman
Customer Service Representative
cfeinman@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

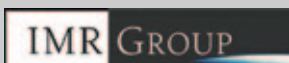
Advertisers in This Issue:

AVON Protection
Bruker Detection
GovSec & U.S. Law Conference
Envionics USA
ICx Technologies
Idaho Technology Inc.
MSA
PROENGIN Inc.
Remploy Frontline

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

DomPrep Journal is electronically delivered by the IMR Group, Inc., 517 Benfield Road, Suite 303, Severna Park, MD 21146, USA; phone: 410-518-6900; fax: 410-518-6020; also available at www.DomPrep.com

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



HAZMAT IDENTIFICATION. IN THE PALM OF YOUR HAND.



Ground-breaking Raman technology in an affordable, palm-size instrument for rapid identification of unknown materials.

Fido® Verdict™ provides real-time, accurate identification of unknown liquids, powders and solids for HazMat professionals. With Verdict, the capabilities of Raman technology are available in an easy to use, miniaturized system at an affordable cost. Hazardous materials identification is now within reach for the entire first responder community.

Contact ICx Technologies at 1-877-692-2120 for more information on Verdict and the Verdict HazMat-CB Responder Kit which includes enzyme-based chemical agent tests and bio-assay strips for a comprehensive chem bio solution.

www.icxt.com

NEW THREATS.
NEW THINKING.®

icx®
technologies

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

A Preparedness Challenge

Transitioning Resilience from Theory to Reality

By Dennis R. Schrader, CIP-R



Working professionals in the Domestic Preparedness community are already familiar with the once vague term “resilience” – but will soon learn more. A lot more – primarily because resilience seems to be an increasingly important component of the Obama administration’s national security strategy, particularly in the area of homeland security.

The White House has, in fact, already created a high-level group to explore the concept in much greater detail. Coincidentally, last month, Philip Palin outlined an argument – in *Homeland Security Affairs* – that the U.S. “Grand Strategy” for Homeland Security should be focused on resilience.

Much earlier than that, though – i.e., in 2004 – Dr. Steven Flynn was an early activist in developing the theory that the resilience of the nation’s infrastructure should be a key security strategy. He and others raised the consciousness of homeland security and emergency management professionals.

The fact is that great endeavors require not just vision, but also human and financial capital – as well as a compelling drive over many years to turn the vision into reality. If resilience is going to transition from theory to reality, therefore, the nation’s engineering and financial communities will have to work together in a meaningful long-term effort. Engineers in particular will have to become more integrated into homeland security and to learn much more about emergency management structures and processes.

The Department of Homeland Security’s Science and Technology Directorate (DHS S&T) has already completed some important preliminary work on the importance of resilience, and recently sponsored an interesting study (*An Operational Framework for Resilience*) that was released in August 2009 by the Homeland Security Studies and Analysis Institute. That study examined not only the “hard infrastructure” but also the “soft operational components” of resilience – including topics such as individual preparedness that contribute to business continuity.

Moreover, in a July 2009 paper presented at Columbia University, Mitchell Erickson of the S&T directorate examined the issue of engineer and scientist roles in resilience efforts – and also pointed out that resilience is and should be a capital cost that has to be justified on a project by project basis.

Meanwhile, the National Infrastructure Advisory Council (NIAC) developed and published a practical report (in September 2009) that examined resilience as “necessary for government and business to create a comprehensive risk management strategy.” In that report, the NIAC concluded that current market forces may be inadequate to achieve resilience for high-consequence/low-probability

events because the business case for investments by the private sector cannot be justified. The report also argued for market-based incentives to encourage resilience.

ASCE's Role; the NIAC Report; And Market-Based Incentives

Engineers will have to become more sophisticated as risk managers during project development. This idea has been advocated by the American Society of Civil Engineers (ASCE) in two of its own studies: "Guiding Principles for National Infrastructure"; and "Vision 2025."

The need for and use of market-based incentives are, in fact, the crux of the issue. The challenge is that infrastructure resilience is still not a well defined, and well understood, area of practice and expertise. Resilience is, though, a design outcome that, as observed in the NIAC report, "complements infrastructure protection" and therefore requires a thorough analysis of interdependencies between infrastructures.

The private sector has begun recognizing that infrastructure resilience is more than just a matter of security, but is also the foundation of the nation's economic prosperity. That recognition led to creation of The Infrastructure Security Partnership (TISP), which was formed by eleven professional and technical associations, and federal agencies, not long after the 9/11 terrorist attacks and since then has been a strong advocate of practical engineering-oriented resilience strategies in both the public and private sectors.

Complementing the TISP efforts, ASCE has been producing an "infrastructure report card" for several years. Resilience was added as a factor in the most recent (2009) Report Card. The bottom line of all of these initiatives can be described in just a few words: Achieving Resilience will be a journey – not a destination. For that reason:

- It will require a collaborative effort that brings engineers and business owners/operators as full partners into the Homeland Security and Emergency Management "Community of Professionals."
- It also will require the appropriate government agencies to re-examine the overall Preparedness Process, with special focus on such important and interrelated topics as

Mitigation, Protection, Recovery, and Resilience – which should collectively be viewed as a systems engineering challenge rather than as separate functional elements.

- Most important of all, perhaps, it will require private-sector governance boards and financial institutions to develop, and effectively use, metrics that value resilience as a major priority.

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

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

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



Registration Includes:

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

The #1 Online Resource for the Preparedness & Response Community



Port Recovery in Haiti: The Initial Stages

By Corey Ranslem, Coast Guard



The 12 January earthquake in Haiti destroyed many of the buildings, including infrastructure facilities not only in Port au Prince, the Haitian capital, but also in the numerous towns and villages surrounding that city; millions of people were left homeless and hundreds of thousands were killed (and/or missing and presumed dead). The buildings and infrastructure of the main cargo port in Port Au Prince also sustained major damage and were closed indefinitely. Most of the piers in the port also were destroyed and most if not quite all of the port's cargo cranes had toppled into the water. In short, the port was useless, and likely to remain so for a long time to come.

Joseph E. Farrell Jr., president of the Resolve Marine Group, saw the damage that had been done to the port, and to the city, and felt compelled to act. "We had a ship heading from Fort Lauderdale to its homeport in Alabama, and decided to turn it around and bring it back to Port Everglades to take on fuel and supplies before heading to Port au Prince," Farrell later commented. "I had seen this type of damage before and didn't want to waste any valuable time."

Farrell had no contract at the time, and had not been hired by any private or government agency, but he decided to fuel his ship, load it with salvage equipment and relief supplies, and get underway for Port au Prince as soon as possible. He knew that the port had to be opened in order for the huge shipments of relief supplies needed – and many tons of it already loaded aboard on an ad hoc flotilla of relief ships – to get into the hands of the suffering Haitian people. Farrell and his Resolve team had previously been involved in other large-scale disasters, and had spent considerable time working in New Orleans in the aftermath of Hurricane Katrina.

Devastation, Destruction, And Both Short- and Long-Term Damage

Nonetheless, they simply could not believe what they saw when they arrived in Port au Prince. "We arrived ... [there] on January 23rd and were astounded at the devastation we saw," Farrell said. "The private port and the main public port in Port au Prince ... [had been] rendered completely useless and the city's infrastructure was completely destroyed. We knew we needed to get the ports operational as quickly as possible."

EXPOSE CHEMICAL HAZARDS



AP4C

HANDHELD CHEMICAL ALARM DETECTOR

- Single-handed Operation
- No On-Shelf Cost
- Fast Start & Recovery
- Fast 2 Minute Response
- Simultaneous Detection
- Easy Operation
- Portable Compact Design
- Rugged Construction



ADVANCED SPECTRO-PHOTOMETRY DETECTS

Nerve, Blister & Blood Agents, TICs & TIMs, Vomiting Agents, Homemade Agents, Hydrocarbons, Precursors

PROENGIN

www.proengin.com

(954) 760-9990

e-mail: contact@proengin.com

The Resolve team, led by Farrell, started immediately working on Port Varreux, just north of the city's main port. Once on scene Resolve was hired by the owners of Port Varreux. Within five days Port Varreux was semi-operational and able to receive a limited amount of fuel and other cargo. The Resolve team established a 400 foot landing zone along the beach to accept cargo from small landing craft. The Farrell-led team, working on contract with Crowley Marine and Titan through the U.S. military/Transcom, turned its attention to the main port to organize the short- and long-term repair process. It was impossible to drive on the docks in the main port, Farrell later recalled, "because most of the pilings were sheered, the docks were broken apart, and the major cargo offloading crane also had fallen into the water." An estimated 95 percent of the docks in the port, he continued, had been damaged or destroyed, "so we knew ... [it] was going to be a long-term project to get the port operational."

An All-American Effort And Private-Sector Assistance

Farrell and his Resolve Group team and Crowley/Titan worked closely with the U.S. Coast Guard and other American naval and military units that had been deployed to Haiti to determine what would be the most effective plan of action.

"Once we had the landing zone in place in Port Varreux," Farrell said, "we started working to clear the containers and cranes from the water and [to] repair the damaged docks in the main port. We [also] worked with Crowley Marine and Seacor to get the port and fuel system online."

Security has been a major concern of almost all of the relief agencies and private-sector companies working in Port au Prince and the surrounding area. The Resolve Group team experienced no security problems in the early stages, though, Farrell said, and the Haitian people have been extremely appreciative of the job the Resolve team and other organizations are doing. His team realizes, Farrell said, that full recovery is going to be a long-term project and will require a partnership with the Haitian government, and the Haitian people, because the long-term "fix" could take up to ten years.



Main cargo moving crane in Port au Prince. The crane and the pier were destroyed during the January 12th earthquake. Resolve Marine is working to have this crane removed before beginning to work on the piers.

Photo Courtesy of Joe Farrell, President, Resolve Marine

"This is not going to be a short-term fix," Farrell said. The Haitian government should "consider building a new port," he added, "because it is going to be very difficult to repair the damage" caused by the earthquake to the former port and its surroundings.

Resolve Marine Group is currently working with Crowley Marine and other companies to get the current port's main cargo crane out of the water sometime in late February. Most of the companies and government agencies involved in the port-recovery effort are using barges to offload cargo into the still crippled port, and at the same time are seeking to get more barges in place to offload as much additional cargo as possible. Through their efforts, more than 1,000 containers loaded with relief supplies had already been moved ashore by the second week of February. So a great deal of progress has in fact been made – but everyone involved recognizes that much, much more remains to be done.

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. He holds a Bachelor's Degree in Communication and Political Science from the University of Northern Iowa, an MBA in International Business from Georgetown University, and has almost 15 years of experience in maritime law enforcement and security.

WE REDUCED THE SIZE. NOT THE PROTECTION.

NIOSH
National Institute for
Occupational Safety and Health
CBRN



NH15
ESCAPE HOOD



AVON
PROTECTION

1 888 AVON 440
www.avon-protection.com

Has Resilience Become the New Protection?

By Leslie-Anne Levy & Monica Giovachino, CIP-R

The recent release of the first *Quadrennial Homeland Security Review* (QHSR) marks a key milestone in the evolution of homeland security. Like most strategic documents, it provides a valuable framework for long-term action by first defining the issue and then articulating the missions, goals, and objectives for improving homeland security. But on a more basic level the QHSR gives a snapshot of current thinking about the definition of homeland security and its guiding principles. As the latest entry in the constellation of homeland security doctrine, the QHSR allows the community to start to discern trends that have emerged during this first decade of what in the future may accurately be described as the homeland security era. The perspective provided by the QHSR shows not only how far the United States has come in its thinking about homeland security, and what debates have been settled to date, but also what major issues must still be resolved.

An important example of the latter involves the missions of critical infrastructure protection and resilience. Protection is defined as the actions or measures taken to cover and/or shield from exposure, injury, or destruction. Resilience refers to the ability to resist, absorb, recover from, and/or successfully adapt to adversity or a significant change in previous conditions. Within the overall field of homeland security, the policy focus to date has been primarily on the protection of the critical infrastructure assets and systems that provide essential services. But resilience has rapidly emerged as a still relatively new theme in homeland security, setting up a debate on how the closely intertwined but very different concepts of protection and resilience relate to one another.

The first *National Strategy for Homeland Security* included protection and security as core pillars of its initial framework. That seminal document, issued less than one year after the 9/11 terrorist attacks, defined – for the first time – what homeland security really means and what it would and should become. Understandably, terrorism was the principal focus of the National Strategy – which spelled out in considerable detail the primary national objectives centered on: (a) preventing ad-

ditional terrorist attacks within the United States; (b) reducing the nation’s vulnerability to such attacks – and to terrorism in general; and (c) recovering from any future attacks that might nonetheless occur. In what was perhaps a telling sign of the times, the word “resilience” did not appear anywhere in the first iteration of the national strategy – an absence that seems rather strange in today’s environment, where resilience has become a popular buzzword.

Within the overall field of homeland security, the focus to date has been primarily on the protection of critical infrastructure assets, but resilience has rapidly emerged as a still relatively new theme, setting up a debate on how these closely intertwined but very different concepts of protection and resilience relate to one another

Moving Forward – In an Era of Constant Change

Today, in 2010, resilience is suddenly everywhere, both as a mission and as an organizing framework. This shift in public awareness was undoubtedly driven in part by the long road to recovery experienced after Hurricane Katrina, and will be further shaped by the lessons learned from last month’s earthquake in Haiti. Earlier this year, the QHSR cited resilience as one of three key concepts that form the general foundation for a comprehensive approach to homeland security, and in September 2009 the National Infrastructure Advisory Council delivered a report to the President on critical infrastructure resilience and offered a series of policy recommendations on the issue. Moreover, several recent books – e.g., *The Age of the Unthinkable* by Joshua Cooper Ramo, *The Edge of Disaster* by Stephen Flynn, and *The Unthinkable* by Amanda Ripley – also

dissected the issue of resiliency, and, of perhaps greater importance, framed several possible strategies for making the critical U.S. infrastructure, the American people, and the nation at large more resilient.

But the relationship between protection and resilience in homeland security has yet to be fully defined or explained. And a major question has yet to be answered: Is one mission a subset of the other, or are they equals? The latest version of the National Infrastructure Protection Plan (NIPP) describes protection as covering a range of activities, including not only traditional security functions – such as improving security

protocols, hardening facilities, and installing security systems – but also actions that are more resilience-focused (e.g., building resiliency and redundancy, and business continuity planning).

Assembling this rather broad spectrum of activities under the same umbrella, protection, implies at first glance that resilience is a component of the overall protection mission. However, protection and resilience also can be framed as complementary elements of a broader approach to managing risk, as the NIPP also begins to suggest. Rather than seeing one as a subset of the other, they can be viewed as linked concepts: infrastructure protection covers what is done to stave off an event and/or limit its damage, while resilience is about minimizing the disruptions that follow the event. Viewed in this context, they become reinforcing components of a holistic approach to managing risk that involves deterring threats, reducing vulnerabilities, and mitigating the consequences associated with a terrorist attack or other incident. Seeing protection and resilience as equals may help foster better integration of critical infrastructure in traditional preparedness activities – planning, training, and exercises – that help build resiliency.

Regardless of how these complementary relationships are ultimately defined – in official or unofficial terms – the reality is that both protection *and* resilience must continue to be part of the homeland security business model moving forward. There is no way to effectively protect the United States, or the American people, against every possible adverse event. For that reason alone, public agencies at every level of government, businesses both large and small, and everyday citizens must be able to absorb, adapt to, and recover from both major disasters and temporary disruptions. In short, the threshold of what must be withstood through improved resilience can be lowered through the application of smart protection and security actions – ahead of time, in the places that matter most.

Leslie-Anne Levy is an Associate Director in the CNA Safety and Security Center. She currently leads a FEMA-sponsored project at CNA developing homeland security risk management training for state and local personnel, which is available at no charge at www.LearnAboutRisk.com.

Monica Giovachino is the Safety and Security Center Managing Director at CNA, a non-profit research organization that provides analyses and solutions to public-sector organizations. She directs CNA's research activities in homeland security, emergency management, public health preparedness, and criminal justice.

Anytime... Anywhere

Solutions, Lessons Learned, Best Practices

The #1 Online Resource for the Preparedness & Response Community



DomesticPreparedness.com

DPJ Weekly Brief

DomPrep Journal

Free access to restricted channels • Robust archive of articles • Huge calendar of events
Peer-to-peer practitioner writers • Interactive - NEW comment section • Over 20 channels of content
Newsletter emailed every Wednesday

FREE registration at <http://www.DomesticPreparedness.com>

P.O. Box 810 • Severna Park, MD 21146 • USA • Phone: 410.518.6900 • Fax: 410.518.6020 • Email: info@domprep.com



GPS-Equipped Vehicles and the EMS Infrastructure

By Joseph Cahill, EMS



One of the principal components of the emergency medical services (EMS) infrastructure is the fully equipped ambulance. But a number of other vehicles, such as paramedic “fly cars” – vehicles that are used by paramedics to respond more quickly

to the scene of an accident, but are not themselves capable of transporting a patient – and various support and supply vehicles also are of increasing importance. EMS units everywhere perform a number of common functions – including, for example, providing treatment during transportation. Realistically speaking, though, many if not most EMS units are poorly equipped to provide long-term care at a fixed location. For that reason, the EMS vehicles lacking the capability to provide transportation are used for other purposes.

Many modern EMS agencies use advanced GPS (Geographic Positioning System) technology to track their vehicles. The GPS systems include a device, mounted to the vehicle, that collects signals from satellites in orbit high above the earth. By comparing its current position to the positions of a number (three or more, usually) of these highly sophisticated satellites the GPS system can determine with astounding precision – through the use of extremely sophisticated geometric calculations – its own location on the earth.

The EMS GPS system differs in several important ways, though, from the GPS systems that many everyday citizens now use to find their way around and/or to travel from one city to another in that the EMS device also can communicate back through the satellite system to a base computer. In many communities this capability allows messages from the base to be forwarded in real time to the vehicle operator.

Judicious Rationing & Other Ancillary Benefits

Many EMS fleets, particularly those in larger metropolitan areas, use the GPS devices to ensure that the vehicle nearest to the scene from which a request for assistance has been received can be quickly determined by comparing the probable travel distances of several vehicles in the same general area. Obviously, anything that speeds the resource to the need translates directly into more lives saved that might otherwise have been lost.

On a “routine” working day this capability not only reduces the EMS response time but also allows system managers to shift some vehicles to areas where resources may already have been depleted. An added benefit is that the system managers

also have greater assurance that their units are where they are supposed to be. The overall improvement in productivity is sufficient reason in itself, of course, to purchase the GPS unit, because it keeps overall system costs down by helping the EMS agency use its resources most efficiently.

There are, however, several additional gains that are realized, but not always recognized. When a major traffic accident or other incident occurs, for example, the closest units can be dispatched to assist, as is done in responding to more routine incidents. In most cases, though, all first responders in the area want to assist in the response. For practical and operational purposes, however, not all of the responders within driving distance can or should be allowed to respond – for two reasons.

The first reason is that there is a “tipping point” beyond which additional resources start to crowd each other out. The second reason is that, if all the resources available in a fairly large geographic area are deployed to the same incident scene, there would be none left to respond to the routine calls for assistance that will still come in from other locations in the same area. When a major incident does occur, therefore, the careful husbanding of what are usually scarce resources in any case allows better management of the overall EMS fleet. Moreover, in the event of a truly overwhelming disaster the “rationing” approach may be the only way to locate unstaffed vehicles. Also, at a time when any vehicle might quickly become a truly life-or-death resource, the imposition of judicious limits on vehicle use may help bring the entire fleet back on line at a faster clip.

An additional point worth consideration: Because communications to and from the vehicle are via satellite, the catastrophic loss, in whole or in part, of the local community’s communications infrastructure – e.g., cell towers, radio repeaters, and trunking systems as well as phone lines – is immaterial to the effectiveness of GPS-equipped vehicles. For that reason, a system purchased to improve productivity on a day-to-day basis also can help: (a) to maintain control over limited resources during a major incident; and (b) to assist in re-forming the system during or after a truly catastrophic disaster.

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.

No Easy Choices in Coping With a Nuclear Gorilla

By Neil C. Livingstone, Viewpoint



This year's Herzliya conference in Israel has just concluded. The three-day conference on Israel's security, which drew nearly a thousand participants, was both wide-ranging and intense.

Although only a few of the speeches and panels directly addressed the issue of Iran's nuclear program, Iran was the eight hundred pound gorilla behind the scenes in every session.

To say that Israelis are paranoid when it comes to Iran and its fanatical president Mahmoud Ahmadinejad, who seethes with hatred for Jews and Israel, is an understatement. Although the Obama Administration and America's milquetoast allies in Europe debate endlessly as to whether or not Iran has nuclear weapons – or the ability to enrich uranium to the threshold level needed for a bomb – Ahmadinejad announced on February 11, at the 31st anniversary of the Islamic revolution, that Iran had become “a nuclear state.”

Anyone who believes that Iran's nuclear program is for peaceful purposes is either a fool or an Iranian dupe.

And the Israelis know that time is running out: If the Iranians do not have a bomb and a workable delivery system today they soon *will* have both. In addition to possessing the ability to launch a missile attack, Tehran can always provide a nuclear device to a terrorist group – which could then smuggle it into one of America's great cities and detonate it. Or it could be used, with devastating effect, as the warhead of a short-range missile launched from a rusty freighter lying in international waters off the U.S. coast. The conclusion is obvious: If the United States or Israel wants to do something about the Iranian nuclear program, the window of opportunity is extremely small and narrowing with every passing day.

A Casual Comment at a Memorable Lunch

A few years ago this author had an informal lunch in Jaffa with a high-ranking former Israeli general and a former head of the Mossad. In Israel, former military and intelligence officials tend to be traditional Labor Party supporters, rather than adherents of the right-wing Likud or one of the minority parties – in large measure because ultra-Orthodox Jews, one of the key constituencies of Likud, do not generally serve in the military or spy services, and are specifically exempted by law if they are studying full time in seminaries. The general who was my lunch companion leaned over and said to me, “The only question [Israel's major political

parties] are united on is Iran. We can absorb only one hit, and we cannot permit that to happen.”

Israel and the United States are rapidly running out of options regarding Iran and the future of its nuclear program. It already is known that Iran possesses intermediate-range missiles capable of carrying a nuclear warhead to Saudi Arabia or to the southern rim of Europe. Not wanting to repeat the mistake Iraq made when it built the above-ground Osirak nuclear reactor – which was bombed by Israel in 1981 – the Iranians have buried their enrichment and other

nuclear facilities (at least 16 major sites and as many secondary sites) deep underground. It is now questionable whether all of those sites could be destroyed, even with U.S.-made 30,000-pound bunker busters capable of burrowing far into the earth. As U.S. General David Petraeus has observed, “Well, they [Iran] can certainly be bombed. The level of effect would vary with who it is that carries it out, what ordnance they have, and what capability they can bring to bear.”

The consequences of launching a preemptive attack on Iran, either by Israel or the United States, are troubling at best. Even if Iran's nuclear program were substantially crippled or totally destroyed, the Iranians would simply start over again – and, because of the knowledge and experience they have already amassed, they could rapidly reestablish their nuclear



program. Moreover, in retaliation for an attack, the current regime in Tehran would probably, like a wounded and cornered bear, activate its terrorist resources around the globe and throw them at Israel, the United States itself, and U.S. allies – especially the conservative Arab regimes in the Gulf. Iran is governed by a Kamikaze regime and could reasonably be expected to do everything in its power to make the United States pay, and pay dearly, for any preemptive actions taken against Iran.

One also can assume that both Hamas and Hezbollah would launch massive attacks against Israel. Iranian-backed terrorists also would target American embassies and business around the world, and might conceivably carry out attacks in the United States more deadly and debilitating than those suffered on 9/11.

Iran already has threatened to attack the Arab states in the Gulf and to block the Strait of Hormuz at the mouth of the Persian Gulf, which is only 29 miles wide at its narrowest point and through which 20 percent of the world's oil passes. Oil prices would skyrocket and petrol shortages could immobilize entire nations. Numerous already weakened economies could be expected to tighten even more, throwing tens of millions out of work and devastating major stock markets around the world.

Several Options – None of Them Good

New economic sanctions are unlikely to dissuade Iran from pursuing its nuclear ambitions, and Russia and China are major question marks in terms of their support for more stringent sanctions. The only sanctions regime likely to work, in fact, would have to isolate Iran completely – both economically and politically – from the rest of the world. That option, of course, would have its own risks.

Nonetheless, if the decision *is* made to attack Iran, the goal must be regime change, and not simply the disruption of the Iranian nuclear program. There have long been tensions between Iran's military and the Revolutionary Guards, which serve as the private army of the mullahs and not only receive the newest and best equipment but also operate businesses that dominate whole sectors of Iran's economy. Probably one of the best solutions, therefore, would be to support an army seizure of the government by someone, or some group, ruthless enough to purge the government of the mullahs and their followers. Any preemptive attack on Iran is likely to have far-reaching and grave consequences. The same can be said, though – even more emphatically – for *failing* to act and thereby permit-

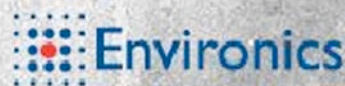
ing Iran to obtain nuclear weapons. Either way, U.S. intelligence agencies – as well as the nation's law-enforcement, first-responder, and homeland-security communities – must begin making immediate contingency plans for the worst-case scenarios likely to develop from whatever decisions are made to deal with the Iranian conundrum.

Dr. Neil C. Livingstone, chairman and CEO of Executive Action LLC and an internationally respected expert in terrorism and counterterrorism, homeland defense, foreign policy, and national security, has written nine books and more than 200 articles in those fields. A gifted speaker as well as writer, he has made more than 1300 television appearances, delivered over 500 speeches both in the United States and overseas, and testified before Congress on numerous occasions. He holds three Masters Degrees as well as a Ph.D. from the Fletcher School of Law and Diplomacy. He was the founder and, prior to assuming his present post, CEO of GlobalOptions Inc., which went public in 2005 and currently has sales of more than \$80 million.



CHEMPROFX

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

The Environics logo consists of a stylized grid of dots in blue and red, followed by the word "Environics" in a blue, sans-serif font.

DomPrep Survey

Your Thoughts Compared with DomPrep40's National Experts on...The Security of National Infrastructure

By John F. Morton, DP40

In our first survey, Domprep members offered their perspectives on the DomPrep40's opinions – compiled earlier this month – on Critical Infrastructure Protection, with special focus on Resilience, a term made prominent throughout last year's National Dialogue on the Quadrennial Homeland Security Review (QHSR) and now in the just-released report – which can be viewed online at (http://www.dhs.gov/xabout/gc_1208534155450.shtm).

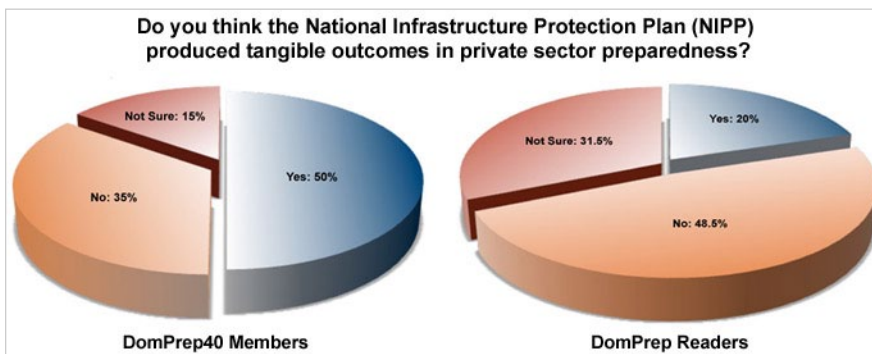
DomPrep40 member Dennis Schrader, the former FEMA deputy administrator for preparedness who prepared this survey, says, "The results are not surprising. We have work to do to create an integrated network of public safety officials and the engineering community."

Key Finding: DomPrep members are more skeptical than the DomPrep40 are about the tangible preparedness outcomes deriving from the National Infrastructure Protection Plan (NIPP) both in the private sector and in state and local public safety agencies.

Also not surprising is the fact that the survey reinforces the DomPrep40's poll results, suggesting that engineers are not, at present, well integrated into public safety planning. For that reason, as both groups – DomPrep members and the DomPrep40 -- seemed to recognize, the public and private engineering communities and public safety disciplines must improve their interfaces.

Here are the survey results:

Significantly more DomPrep members questioned whether the NIPP has produced tangible outcomes in private sector preparedness. A mere one-in-five said that it has, as compared to half of the DomPrep40.



Just under one-in-three members said that, in their opinion, the NIPP has produced tangible outcomes in state and local public safety preparedness. Almost two-in-three of the DomPrep40 agreed. Overall, with regard to the NIPP, DomPrep members were therefore more skeptical of NIPP outcomes.

The DomPrep40

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

DomPrep40 Members

John Morton

Strategic Advisor

James Augustine

Chair, EMS & Emergency Department Physician

William Austin

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

Ann Beauchesne

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

Bruce Clements

Public Health Preparedness Director, Texas Department of State Health Services

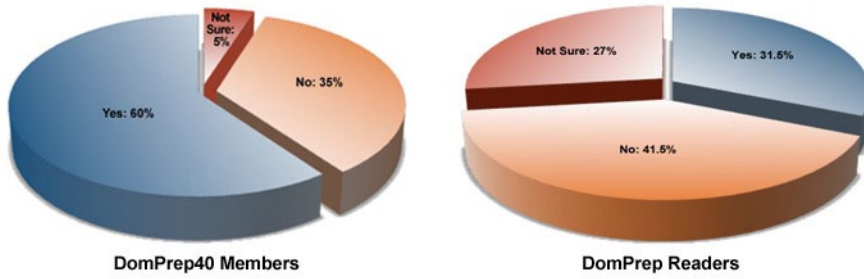
John Contestabile

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

Craig DeAtley

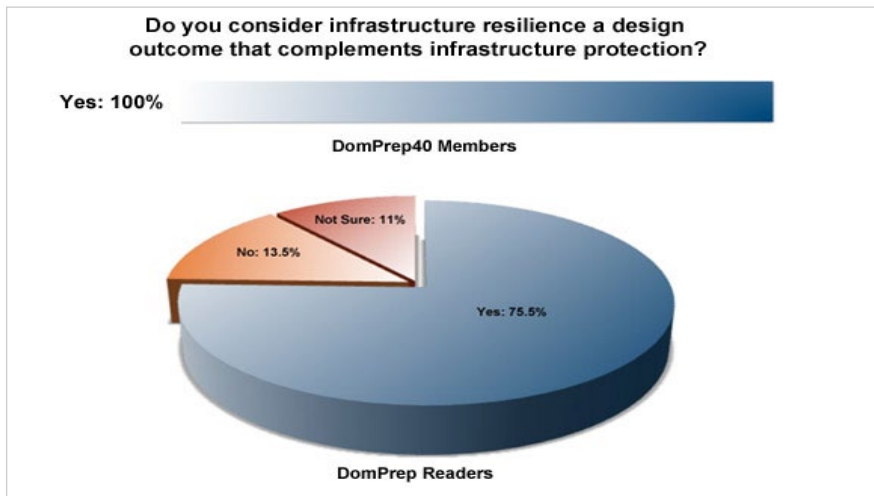
Director for Institute for Public Health Emergency Readiness

Do you think the National Infrastructure Protection Plan (NIPP) produced tangible outcomes in state & local public safety preparedness?



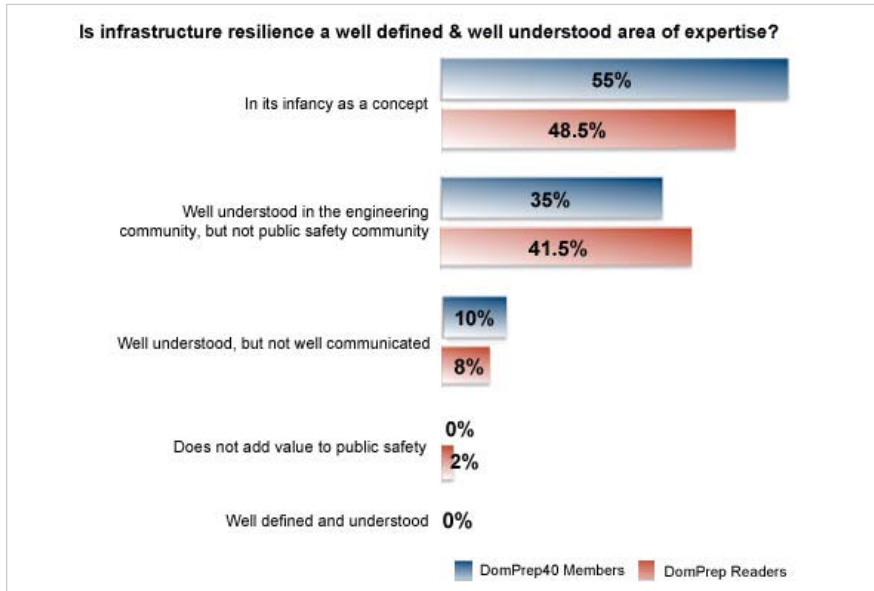
DomPrep members, for the most part, did agree with the DomPrep40 on resilience as a design outcome that complements infrastructure protection; a full three-quarters of them said yes.

Do you consider infrastructure resilience a design outcome that complements infrastructure protection?



DomPrep members also essentially agreed with half of the DomPrep40 that infrastructure resilience as a concept is still in its infancy, but a notable percentage saw it beginning to take root in the engineering community – e.g., in public works.

Is infrastructure resilience a well defined & well understood area of expertise?



DomPrep40 Members

Nancy Dragani

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

Warren Edwards

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

Katherine Fuchs

Deputy Chief FDNY Emergency Medical Services Command

Ellen Gordon

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

Kay Goss

Former Associate Director, National Preparedness Training & Exercises, FEMA

Steven Grainer

Chief, IMS Programs, Virginia Department of Fire Programs

Jack Herrmann

Senior Advisor, Public Health Preparedness, NACCHO

James Hull

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

Harvey Johnson, Jr.

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

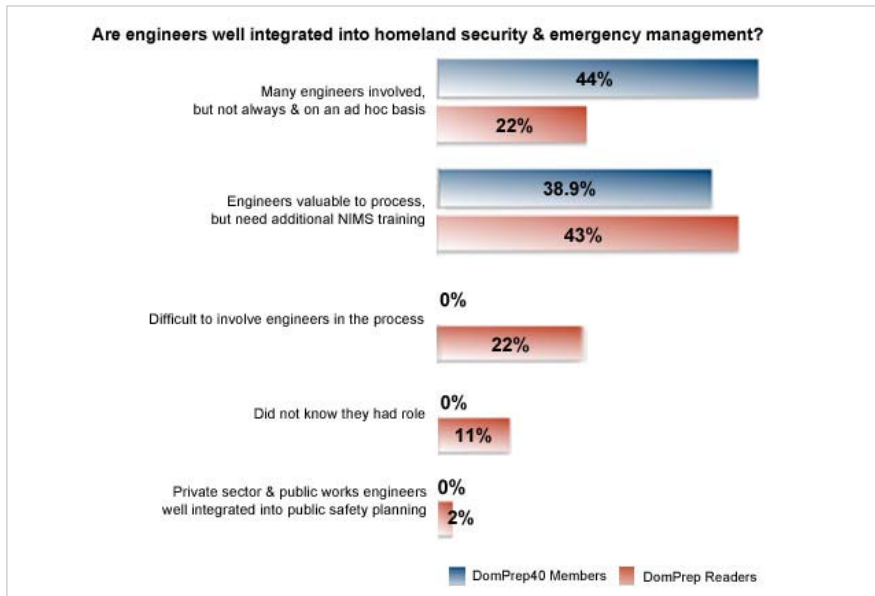
Dennis Jones, RN, BSN

Executive Consultant, Collaborative Fusion Inc.

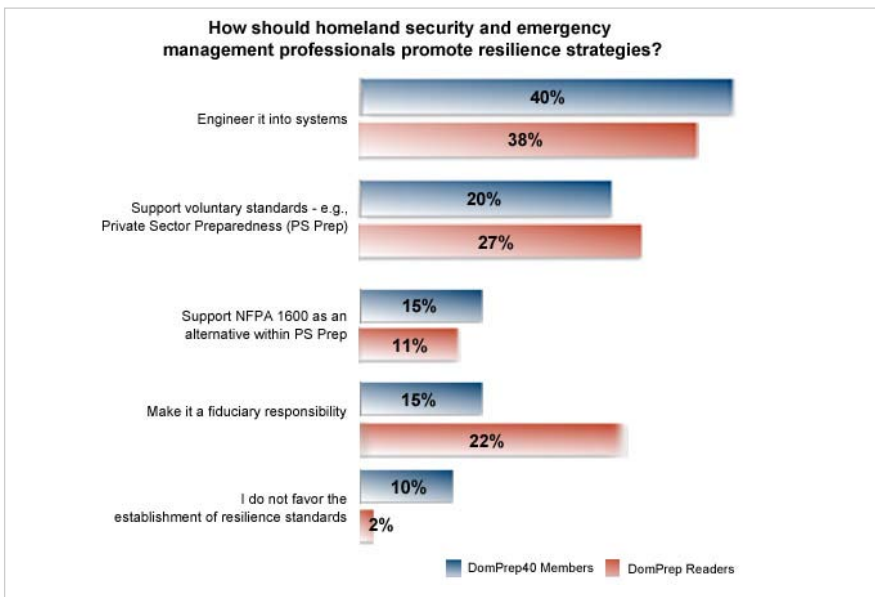
Robert Kadlec

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

DomPrep members emphasized, much more than the DomPrep40 did, their concern that engineers are not well integrated into the professional development programs developed for the National Incident Management System (NIMS).



No surprises here: A mixed card, again, as to how best to promote the implementation of resilience strategies – with a significant minority of members (as was the case with the DomPrep40) saying to “engineer it into systems.”



As was noted in our previous summary, one of the main goals of the QHSR National Dialogue was the establishment of resilience metrics. How implementation will actually progress remains to be seen, of course, but on this last question only two percent of the DomPrep members opposed the establishment of resilience standards.

It is our carefully considered conclusion, based on the inputs received from both the DomPrep40 and DomPrep members, that this representative sampling at least appears to recognize the need to involve engineering more thoroughly in resilience processes and systems in general – and, more specifically, into NIMS training.

DomPrep40 Members

Neil Livingstone

Chairman & CEO, Executive Action

James Loy

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

Adam McLaughlin

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

Vayl Oxford

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

Stephen Reeves

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

Richard Schoeberl

Executive, Federal Bureau of Investigation & the National Counterterrorism Center

Dennis Schrader

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

Robert Stephan

Former Assistant Secretary of Homeland Security for Infrastructure Protection

Joseph Trindal

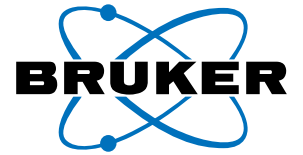
Former Director, National Capital Region, Federal Protective Service, Immigration & Customs Enforcement (ICE)

Theodore Tully

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

Craig Vanderwagen

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



Bruker Detection Corporation



**Early Detection
is the First Step
in Protection**



E²M GC/MS System

- Identifies and quantifies organic substance in soil, air, water and from surfaces
- Mobile, compact, fast and reliable
- Software includes all standard MS acquisition methods
- Use internally purified air as carrier gas – no helium, hydrogen, or nitrogen required



HAWK FR Stand Off Detection

- Detects chemical vapors up to one mile line of sight
- Detects CWAs and many industrial chemicals
- Scan large areas in seconds
- Stand-alone or can be integrated into a network



M-IR Mobile FT-IR

- Wear-free ROCKSOLID™ interferometer for industry leading performance and reliability in harsh environments
- Rugged, portable, self contained solids and liquids analyzer
- Bearing mechanism is space qualified and virtually free from wear
- Easy-to-use graphical user interface; assistant guided operation

(978) 663-3660 x1308 ■ nbc-sales@bdal.com ■ www.bruker.com/detection

think forward

CBRN Detection

Local Security: The Forgotten Factor in Relief Operations

By Joseph Trindal, Law Enforcement



The earth shook and tens of thousands of homes, as well as an estimated 30,000 business and office buildings, were shattered. But the buildings were not the only things to collapse in Haiti. Recognition of the numerous weaknesses in the pre-earthquake Haitian infrastructure would lead the average citizen to expect the need for an extremely complex relief effort. What made that effort even more difficult is that the epic 12 January disaster also brought down the Haitian government's ability to maintain law and order.

For that reason, regional and global disaster relief efforts quickly became a secondary casualty of the ensuing chaos on the ground, especially in the nation's capital of Port au Prince. Only a week after the earthquake, Vincenzo Pugliese, a United Nations spokesman, was quoted in the 19 January *Washington Post* as saying that, "Security is the key now in order for us to be able to put our feet on the ground."

The international community's failure to appreciate the scope of the security challenges facing the relief agencies and organizations that responded so well, and so quickly, was almost as appalling as the earthquake itself. By the close of the first decade of the 21st century, the security requirements for disaster relief operations should be fully integrated into any and all situational response plans developed.

If nothing else, recognition of the Haitian government's already limited security and police-service capabilities should have been factored into the equation as a predictor of the extremely weak post-disaster sustainability likely in support of the relief effort. The rule of thumb should be that the weaker a locale's steady-state security infrastructure is, the more external security support will have to be embedded into the relief operations.

The First Priority: A Realistic Risk Assessment

The weakness of indigenous security capacity is or should be a critical factor in disaster relief planning. Judging from the relief operations in Haiti over the past seven weeks, disaster security planning seems to have been an afterthought. There is a more important lesson to be learned, though – namely, that security services should be factored into *all* disaster planning, ranging from local incidents to those affecting an entire nation or global region. A thorough risk assessment focused primarily on disaster-relief operations should therefore be a prominent core feature of rapid post-disaster planning and deployment operations.

By their very nature, even relatively "minor" disasters almost always strain the local resources available. It logically follows, therefore, that the weaker the local security structure is, the more likely it will be that external security elements will be needed to protect not only disaster supply stores and distribution chains, but also, and of greater importance, the disaster-relief personnel themselves.

Disaster relief planning, particularly in the 21st century, must also consider the possibility of extreme post-disaster threats. When the in-

ternational community responds to a disaster, the relief assets provided become potentially accessible targets for transnational terrorists and local insurgents alike. The disruption of disaster-relief operations is an attractive temptation to malicious groups seeking to propagandize response incompetency and to perpetuate fear in the affected population. Such attacks, followed by propaganda messages, would rapidly degrade public confidence in government both within the affected area and in the nations involved in the relief operations.

Situational Violence to Compound the Chaos

Criminal and terrorist attacks designed to thwart or disrupt disaster relief efforts undermine the volunteer support for, and capital investment in, disaster relief operations. An organization or government engaged in relief operations in which its own personnel and/or material resources are jeopardized may lose both its capacity and its willingness to support future operations. For the United Nations itself to underestimate the number and types of peacekeeping forces needed in Haiti is a disturbing indicator of future potential problems of even greater magnitude.

Disaster relief operations can be effective only if the operations being carried out, and the personnel participating in those operations, are provided a safe environment in which to carry out their mission. The capacity for local resources and the degree to which augmentation by external security forces will be needed should be standard, high-priority elements in disaster operations planning. Government and private-sector relief efforts should factor security requirements into the cost and staffing models for all disaster relief operations.

The degree to which external security assets are needed is always a situational variable. Any failure to accurately assess and provide for the security needed is therefore unacceptable. The compounded disasters in Darfur and Somalia – to name but two of the most difficult, and better publicized – international problem areas in recent years, illustrate the adverse effects of the secondary disasters that can quickly be created by insufficient security support. With proper planning, though – in which security requirements are fully and appropriately given very high priority – disaster management can and usually will provide the relief necessary, rather than compounding the original disaster.

Joseph Trindal is the Managing Director at KeyPoint Government Solutions Inc., and 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.

The Principles of Infrastructure Resilience

By Scott Jackson, CIP-R



Resilience, as described in 2007 in documents related to the Critical Infrastructure Protection (CIP) Program, is broader than protection in that protection focuses primarily on survival. Resilience includes plans for the recovery and continued functioning of the infrastructure even if some elements of the infrastructure do not survive. Resilience takes some of the pressure off protection, and allows for recovery even when total protection is not feasible. It also considers how a building, power plant, or other component of critical infrastructure is prepared and protected, whether responders and/or the community at large can take advantage of advance warnings, and whether there are alternative plans in place for continued operation. Resilience also takes into consideration whether those whom responders depend on also are likely to survive and recover.

Resilience has become a subject of increased interest in recent months, at least partly because both the Department of Homeland Security and the Obama Administration have adopted resilience as a primary focus area. Resilient infrastructures can anticipate, survive, and recover from external disruptions, such as terrorist attacks – and from natural disasters, such as hurricanes and earthquakes. Resilient infrastructures also can recover from internal disruptions, such as human and software errors. Infrastructures that are *not* resilient are called brittle. Fortunately, a world-wide community of scholars, researchers, and decision-makers has made significant strides in defining resilience and developing its guiding principles.

First, an infrastructure can be seen as a system. Systems are collections of parts, called elements or nodes, that together have a common purpose. The common purpose of a transportation infrastructure, to consider but one example, is to carry people and cargo across various distances. The purpose of a power infrastructure is to provide power to residences and industry throughout a fairly large area.

Similar infrastructures exist for a community's water supply, fire protection, healthcare, defense, communications, and law enforcement. Because each of these infrastructures is almost always separately owned and managed – but also dependent in varying degrees on the other infrastructures – the whole

is sometimes called a system of systems. The U.S. *national* infrastructure itself is a system of systems.

Some components of the U.S. national infrastructure – railroads and airlines, for example – are privately owned and managed. Other parts are government agencies, such as fire and police departments. One of the major challenges facing U.S. decision makers and emergency managers, at all levels of government, is how to make the national infrastructure more resilient.

The Architecture of an Infrastructure

The term *architecture* is used to describe how the various parts of an infrastructure are arranged and relate to one another. The creation of an architecture is sometimes called *architecting*. The architecting process asks, and seeks answers to, a number of questions, including the following: (a) How many modes of transportation should there be? (b) How can the nodes of a power infrastructure be arranged so that the loss of one node will not cause the entire power infrastructure to cease functioning? (c) How can and should a private or government infrastructure reorganize to survive and recover? The following review of the four principles of resilience – capacity, flexibility, tolerance, and cohesion – answers those and a few other questions.

The first and perhaps most important principle – **capacity** – is that all infrastructures have, or should have, the capacity to withstand “known” disruptions, such as hurricanes and floods. Capacity includes not only the ability to absorb such disruptions but also a margin of additional ability to cope with disruptions larger than anticipated. Capacity also includes both physical and functional redundancy so that the infrastructure will have alternative ways to survive. Functional redundancy could mean, for example, that a coastal city would have several possible ways for the local populace to evacuate the disaster area and find shelter elsewhere. Those ways could and probably would include the use of cars, trains, boats, aircraft, and other modes of transportation. Obviously, the more “ways” there are to evacuate, the more resilient the infrastructure is.

Unfortunately, there are several fairly recent examples of infrastructures that did *not* meet the capacity test. The 2007 collapse of the Minneapolis-St. Paul bridge, and the collapse of several New Orleans levees during hurricane Katrina in 2005, are perhaps the most obvious of those examples. The

**FIRST RESPONDERS NEED TO BE
PREPARED FOR ANYTHING...**



For expert and informed discussion on
how to face your CBRN threat contact:

USA Tel: +1 866 803 5956 (Toll Free)

Email: frontline@remploy.com

UK Tel: +44 (0)845 241 2990

Email: frontline@remploy.co.uk

www.rememployfrontline.com

SO DO OUR SUITS

Remploy Frontline

SURVIVAL EVOLUTION

long-term stresses on the bridge, and the overflow heights of the levees, were well known long before disaster struck. The principal readiness shortcoming was that the capacity required was not maintained – or, preferably, augmented – after the infrastructure elements were built.

The capacity example provided last year by US Airways Flight 1549 was somewhat different. There is no evidence to date that the Airbus airplane did not meet the Federal Aviation Administration (FAA) requirements for bird ingestion; in fact, the flock of geese that caused the aircraft's engines to shut down exceeded the FAA requirement. Nevertheless, the aircraft "system" – which included the pilot and crew as well as the passengers – survived, demonstrating that it was a *resilient* system.

In contrast, the 2001 attacks on the twin towers of the World Trade Center (WTC) in New York City greatly exceeded the capacity of the two buildings to survive such an attack. Both buildings presumably had the capacity to withstand all *precedented* – i.e., previously known – disruptions. In this case, the recovery of the city itself did not depend only on capacity, but on a number of other resilient factors, such as a supply of generators sufficient to restore power in Manhattan within five hours (as pointed out by David Mendonça and William Wallace in their 2006 report on "Adaptive Capacity").

However, infrastructure resilience cannot depend on capacity alone. Resilience enables infrastructures to recover even when the disruption exceeds the capacity, as in the case of the US Airways flight.

Flexibility: Resilient infrastructures also must be flexible – which means, more specifically, that the infrastructure system should be able to reorganize itself. Once again, the New York Power Restoration case study shows that a major factor in the restoration of power so soon after the attacks on the WTC was the ability of the local power agency to reorganize and focus on deploying generators throughout the city.

Reorganization also includes the ability of the infrastructure to elevate levels of authority during a disruption. Such elevation of authority is particularly common in the fire prevention arena. The San Francisco Fire Department, for example, employs a system in which, as the severity of an emergency increases, the authority rises first from the firefighter level to the supervisory level and then to the senior decision-making level of the government agencies involved.

Tolerance: Resilient infrastructures also are "tolerant" of disruptions – tolerant in the sense that the infrastructure will not immediately lose all of its capability following a disruption, but will degrade gradually. Tolerance depends, to a great extent, on *localized capacity* – which already exists today in certain domains. Many hospitals have their own power supplies, for example, in case the public power supply is disabled because of an earthquake or other major disruption. (However, the current national power grid is an example for which localized capacity is not strong enough.)

Another aspect of tolerance is what is called "loose coupling" – a term which implies, for example, that when one node of an infrastructure element fails, that failure will not immediately propagate to and/or affect other nodes. In the 2003 failure of the power grid in the northeastern United States the lack of loose coupling was evident by the rapid propagation

and geographic spread of the failure. A valuable lesson learned from that failure, though, is that loose coupling will undoubtedly be a high priority in the design and building of future generations of power infrastructures.

Another capability in the tolerance area is what is called *drift correction* – which means, basically, that disruptions can be avoided or at least minimized by awareness of their approach in enough time that corrective or compensatory action can be taken. The use of sensors to warn of an impending train collision is one example of how drift correction can be used to prevent or reduce the harmful effects of an imminent disaster.

Resilience also considers how a building, power plant, or other component of critical infrastructure is prepared and protected, whether responders and/or the community at large can take advantage of advance warnings, and whether there are alternative plans in place for continued operation

Cohesiveness: The resilience of an infrastructure also depends on how well the nodes of the infrastructure relate to one another. In a 2006 report on “essential characteristics” of infrastructures, David Woods refers to those relationships as “cross-scale interactions,” and points out that they can occur on three levels. The first level is communication, which asks, specifically, if the nodes “talk to one another” – a question addressed by Karl Stephan in a 2007 IEEE (Institute of Electrical and Electronic Engineers) publication in which he points out that many of the agencies in New Orleans lacked the interoperability, at the time Hurricane Katrina hit, they needed to communicate with one another.

The second level of cohesiveness is cooperation. Even with no formal ties, the nodes of an infrastructure should possess the initiative, and capabilities, needed to cooperate with one another. During Katrina, the New Orleans agencies were deficient on this level as well. In contrast, the New York Power Restoration accomplishment after the 9/11 attacks was a case in which cooperation was manifest among and throughout the power companies, fire and police departments, and U.S. military forces involved. The third and highest level of cohesiveness encompasses *inter-element collaboration*, which includes formal agreements between the nodes to both help and provide resources to one another.

The development, building, and implementation of infrastructure resilience is difficult for a number of reasons, but primarily because of the large and complex array of government agencies and private organizations involved – all of them representing different nodes of the infrastructure. There is general agreement, though, that no single organization, not even the federal government, should or could orchestrate the entire resilience plan. Independent nodes, such as The Infrastructure Security Partnership (TISP), also can and do play a role – by, for example, facilitating agreements between and among the other nodes.

It is important to remember that very few if any of these nodes or entities possess the financial resources needed to fully implement the more costly aspects of resilience. Installing dual railroad tracks, for example, to achieve a certain degree of *physical redundancy* would be very costly. Priorities need to be established, therefore, in assessing what needs should be funded. Fortunately, some aspects of resilience are practically cost-free. Signing a memorandum of agreement with another agency, for example, usually involves only a relatively small expenditure of administrative costs

– an acceptable price to pay when it is remembered that the main responsibility of *all* of the organizations participating in a resilience effort is to collaborate with one another. To briefly summarize: There is general agreement that: (a) The principles of resilience, as defined by the international community, and described above, can and should be applied to the U.S. national infrastructure and to its principal elements; and (b) The most important priority in this effort is and should be the development of a cooperative approach to implementation.

For additional information relevant to the preceding article and/or closely related topics, see:

Critical thinking: Moving from infrastructure protection to infrastructure resilience. CIP [Critical Infrastructure Protection] Program Discussion Paper Series; George Mason University (2007). Or click on: http://www.resilient.com/download/Research_GMU.pdf <http://www.resilient.com/download/Research_GMU.pdf>

Architecting Resilient Systems: Accident Avoidance and Survival and Recovery from Disruptions, by Scott Jackson (John Wiley & Sons, 2010).

“NTSB [National Transportation Safety Board] Blames Engineer for Crash,” by Robert Lopez, Dan Weikel & Rich Connell (*Los Angeles Times*, 22 January 2010).

“Adaptive Capacity: Electric Power Restoration in New York City Following the 11 September 2001 Attacks,” by David Mendoça & William Wallace *Proceedings of the Second Resilience Engineering Symposium*, 8-10 November, Juan-les-Pins, France 2006.

“We’ve Got to Talk: Emergency Communications and Engineering Ethics,” Karl Stephan, IEEE [Institute of Electrical and Electronic Engineers] *Technology & Society Magazine*, 2007.

“Essential Characteristics of Resilience,” David Woods, *Resilience Engineering: Concepts and Precepts*, Aldershot, UK: Ashgate, 2006.

Scott Jackson is a lecturer in the Systems Architecting and Engineering graduate program at the University of Southern California (USC). His book, Architecting Resilient Systems: Accident Avoidance and Survival and Recovery from Disruptions, was published by Wiley in 2010. He is a Fellow of the International Council on Systems Engineering (INCOSE) and represents USC on The Infrastructure Security Partnership (TISP).

Lessons Learned for Critical Infrastructure

By Andrew Pearsons, CIP-R

In order to ensure the continuous functionality of key systems, the Emergency Services Sector (ESS) should incorporate broad measures for protecting all personnel. Such measures should be integrated into all activities, including incident response, exercises, and training.

Homeland Security Presidential Directive 7 (HSPD-7), issued in 2003, identifies 17 critical infrastructure sectors that the federal government must protect against terrorist attacks. These sectors span a wide range of assets that are key to the continuing functionality of the U.S. political and economic systems. The ESS is one of the more unique areas of critical infrastructure protection. While most of the critical infrastructure sectors place a major emphasis on securing structural assets, such as chemical facilities and government buildings, the ESS focuses mainly on human assets. The millions of specialized and highly trained personnel under the purview of the ESS comprise much of the first responder community, including: emergency management, emergency medical services, fire fighting, hazardous materials, law enforcement, bomb squads, tactical operations/special weapons assault teams, and search and rescue.

Because of the magnitude, variety, and mobile nature of ESS assets, protection measures within this sector must be extensive. In effect, these measures must not only span the duration of an incident, but must also cover routine activities, training, and exercises. Two recent *Lessons Learned* – and posted on *Lessons Learned Information Sharing (LLIS.gov)* – demonstrate the diversity of protection measures essential to the functioning of the ESS.

The first, *Exercise Safety and Health: Providing Appropriate Personal Protective Equipment for Exercises*, highlights the need to appropriately equip first responders to prevent injury. In this case, responders taking part in an operational exercise in Pennsylvania Region 13 lacked a specific flotation device for

law-enforcement participants as well as wildfire gear for firefighters. This added to the risk of injury for exercise participants. While the Lesson Learned specifically references personal protective equipment (PPE) issues during a full-scale exercise, the message clearly applies to real world incidents as well. Supplying ESS personnel with appropriate PPE is a simple and effective means for ensuring responder safety. The Approved Equipment List, compiled by the FEMA Grants Program Directorate, devotes an entire section to PPE that can be procured under numerous grant programs. (More information on approved PPE can be found on the *Responder Knowledge Base (RKB.us)*.)

The international community's failure to appreciate the scope of the security challenges facing the relief agencies and organizations that responded so well, and so quickly, was almost as appalling as the earthquake itself; by [this time] the security requirements for disaster relief operations should be fully integrated into any and all situational response plans developed

The second Lesson Learned, *Point of Dispensing Planning: Establishing Safety Measures for Set-Up and Tear-Down Crews*, provides a less common example of ESS personnel safety hazards. During a full-scale exercise at the Oakland-Alameda County Coliseum, observers noted that some support staff performing physically demanding tasks were not provided with guidance on proper safety measures. The need to ensure the safety of all ESS staff, including those not directly involved in a response, is evident in this Lesson Learned. The ESS is dependent upon specialized personnel to execute the systems for which the sector is responsible. Therefore, an injury to any staff member that prevents that person from performing his or her duties could

hamper the ability of emergency service organizations to function effectively during an incident. For this reason, the ESS protective measures must extend beyond the scope of standard responder safety and permeate all activities undertaken by ESS personnel.

Andrew M. Pearsons is a researcher for Lessons Learned Information Sharing (LLIS.gov), the Department of Homeland Security/Federal Emergency Management Agency's national online network of lessons learned, best practices, and innovative ideas for the U.S. homeland security and emergency-response communities. He received his bachelor's degree in Government from The College of William and Mary.

OUR MISSION YOUR SAFETY

MSA
The Safety Company



SAFESITE® MULTI-THREAT DETECTION SYSTEM

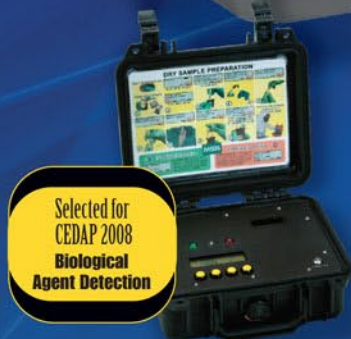
**Critical Infrastructure
Emergency Response
Public Events
Perimeter Monitoring**

*Monitors and wirelessly communicates
6 potential threat types simultaneously:*

- VOCs – volatile organic compounds
- TICs – 16 toxic industrial chemicals
- CWAs – nerve and blister agents
- Gamma radiation



**VISIT US ONLINE
MSANET.COM**



**BIOLOGICAL
AGENT DETECTION**



**CWA & TICs
HANDHELD PORTABLE**



**FIXED-POINT CWA
MULTI-THREAT DETECTION**

1.866.MSA.1001 | www.MSAPOLICELINE.com/domprep.html

Pennsylvania, Kansas, California, and Kentucky

By Adam McLaughlin, State Homeland News



Pennsylvania County Publishes Emergency Call Information Online

In the past, the Montgomery County Department of Public Safety typically received 50-100 calls daily from the local media, most of them inquiring about traffic accidents and/or road hazards that might snarl traffic. To reduce the large volume of phone calls, the department worked with the county's Information Technology (IT) department to develop a web site that – using the county's computer-aided dispatch (CAD) system – provides the public with online information about active fire and EMS (emergency medical services) calls, as well as traffic incidents.

The plan worked so well that the public-safety department has seen an amazing reduction in the number of media calls about traffic accidents and other potential hazards. “There are some days when we might get one or two [calls] in a 24-hour period” – compared to the 50-100 calls in the 24-hour period before – according to Sean Petty, the county's deputy director of public safety for communications and technology. The county's web site, which receives an estimated 60,000 “hits” per month, Petty said, also provides quick information summaries including such data as the incident number, the resources deployed (and/or that have arrived on scene), and the location of the incident – which also is plotted on a Google map. The site also provides a link to the county's “live” EMS and fire-department radio communications systems.

The data that appears on the site is pulled from the county's CAD system every five minutes. As dispatchers enter into the system the information received from incoming calls, the same data is automatically pushed to the web site. “We did not want to have somebody ... [have to] manually approve the incident [data],” Petty said.

In addition to providing the public with an abundance of helpful information, the new system also helps to improve the situational awareness of incident commanders. More specifically, Petty said, “It allows an incident commander or a manager to see where their units are, and when they go on-scene.” It also tells them precisely where an incident has occurred.

Petty's team, working with the county's IT department, also developed a text-only mobile version of the incident status page that allows emergency managers, police chiefs, and fire chiefs to quickly pull up the information on their own mobile devices without having to launch a full web browser.

The county's web site, which receives an estimated 60,000 “hits” per month also provides quick information summaries including such data as the incident number, the resources deployed (and/or that have arrived on scene), and the location of the incident – which also is plotted on a Google map

Petty described the new site as “the most comprehensive” WebCAD site he has ever seen. “Based on the research that I did, and the other sites that I saw,” he said, “I do not know of any other that has all the same features that ours does and is so automatic and gives people the ability to update the events, shows them incident notes, and has the BlackBerry version of it.” In addition, he pointed out, he “did not find any other system that had all of those things in addition to the Google Maps integration.”

Kansas Hosts Conference Addressing Use of Social Media During Disasters

The use of “social media” (Facebook, Twitter, and similar systems) to keep communities, and individual citizens, continuously informed about ongoing emergencies seems to have taken local public information officers by storm, as evidenced most recently by: (a) the national and international increase in use of the social media to stay abreast of the still deteriorating situation in Haiti (many worried citizens used Twitter and other social networks to check on the status and well-being of loved ones); and (b) the use of the same media to help citizens cope with the extremely cold weather and heavy snows

affecting almost all sections of the country during the past several weeks.

The escalating popularity of the social media – with people all over the world, in fact – has led to a number of relevant questions about both the most effective use of the social media and some of the “best practices” that have been learned. Those topics were recently addressed by an estimated 130 or so public and private-sector information officers from the emergency-management, first-responder, and business-continuity communities who gathered in Kansas City on 21 January to participate in the *Midwest Disasters 2.0: Social Media and Emergency Response* training session.

The session’s goal was to assemble emergency communicators from the greater Kansas City area to learn not only how the social media systems work but also how they can be most effectively used during a disaster.

Earlier examples of the social media’s use during disasters, such as the Virginia Tech massacre in 2007 and the Mumbai terrorist attacks in late 2008, spurred the decision to plan and host last month’s session, said Adam Crowe, assistant director of the Johnson County Emergency Management and Homeland Security office. “There seemed to be a growing use of ... [the social media], and then a lot of people in my area of Kansas City were clamoring to learn more,” he said. “Unfortunately,” he added, “the only training [courses] that were popping up were very low-level, basic information about what Twitter is, what Facebook is.”

The best practices “guidelines” on use of the social media to stay informed are unofficial, of course, but have been a major topic of discussion nationwide. However, agreement on what actually constitutes best practices is hard to come by, Crowe said, because so many agencies and communities have developed their own methods for use of the several different social media networks now available. Nonetheless, the *Midwest Disasters 2.0* session provided two excellent examples that illustrated what could and should lead

The boat is designed to scan the contents of a ship through its hull as it is being escorted into port and to transmit the data received to shore-based authorities; [it] also is equipped with a submersible device capable of searching hulls for explosives in zero-visibility conditions

to improved and more effective use of the social media networks.

One example was provided by the local National Weather Service, which uses Skype – a software application that allows users both to make calls over the Internet and to use video conferencing – to talk to the local media before, during, and after a major “weather event.” The other example was provided by one of the local volunteer Medical Reserve Corps chapters, which uses Facebook to improve the effectiveness of its recruitment program. “There were a lot of [other] examples, depending on the system that was used, as to how they [Twitter and other systems] can be best utilized by other people,” said

Crowe, who is responsible for keeping the networks up-to-date.

His own office, he noted, uses Twitter as a free short-message text-notification system. It also uses Facebook, YouTube, and iTunes. Interestingly, Johnson County’s use of the social media started less than two years ago (in 2008) with a blog.

California Los Angeles Adds Screening Vessel, Helicopter to Augment Port Security

The Los Angeles Sheriff’s Office has announced the acquisition, earlier this month, of both a specially equipped boat for screening cargo vessels and a radiation-detecting helicopter aimed at hardening the Los Angeles-Long Beach port complex against future terrorist attacks.

The 55-foot screening vessel is “the first of its kind in the world,” according to a department statement. The vessel and helicopter join a badge-carrying dog, “Johnny Ringo,” that has been trained to “sniff out” chemical and biological weapons.

The boat, valued around \$3 million, and the radiation detection pod for the helicopter, valued at about \$220,000, were paid for by the U.S. Department of Homeland Security, said Sheriff’s Office spokesman Stephen Whitmore. The Sheriff’s Depart-

ment already owned the Eurostar helicopter, he noted, on which the pod is mounted.

Whitmore said that the boat is designed: (a) to scan the contents of a ship through its hull as it is being escorted into the port; and (b) to transmit the data received to shore-based authorities. The boat also is equipped with a submersible device capable of searching hulls for explosives in zero-visibility conditions, Whitmore said.

“The [LA-LB] port complex is one of the most critical infrastructures in the United States,” said Jack Ewell, who was in charge of the upgrading project for the Sheriff’s Department. “Once the ships have been inspected,” he continued, “they are cleared to enter the port complex, where additional security measures are in place” for use by port security officials.

“The screening vessel,” Whitmore also said, “is equipped with highly advanced radiation and chemical/biological detection equipment ... [that] allows deputies to remotely screen entire ships for weapons of mass destruction materials while ... they [the ships being screened] are under way to the port complex.”

The detection equipment can transmit data in real time to the Sheriff’s Department’s hazardous-materials-detail headquarters for further interpretation, Ewell said. The vessel also is equipped with an advanced sonar system that is capable of working at depths of up to 3,000 feet.

The Los Angeles-Long Beach port complex “is the largest and the busiest container port in the United States,” Ewell said. Because 40 percent of all U.S. imports come through the LA-LB complex, he added, “It would cost the U.S. economy [an estimated] \$1 billion a day if the port complex was shut down by an incident.”

Kentucky **Louisville Responders Train to Cope With Radioactive Materials**

Louisville-area police officers and firefighters, Kentucky Air National Guard members, and other public-safety workers donned protective gear earlier this month to practice the handling and disposal of radioactive materials.

The radiation used in the training was low-level, said Metro Emergency Medical Services Director Neal Richmond, but sufficient to provide realistic hands-on experience with the types of equipment, clothing, and procedures that public-safety workers would have to use to deal with a terrorist attack of the kind that could spread radioactive materials over a wide area.

The training, which was conducted at the Pleasure Ridge Park Fire District Training Center, also would be useful in responding to a medical or industrial accident involving radioactive materials. The course was conducted by a branch of the U.S. Office of the Counter Terrorism Operations Support Program, working in cooperation with the state’s own Department of Homeland Security.

The training provided was “a great opportunity,” Richmond said, to develop “an extra level of skill.” He noted that the 25 safety workers who participated in the training had volunteered for the three-day session to help their organizations hold down overtime costs.

An accident involving radioactive materials probably is a more likely threat, day to day, than a terrorist attack would be, Richmond said. It is nonetheless very important for the first emergency workers at the scene of a radiation incident to be fully aware of the risks involved, he said, and to know how to use the detection and protective equipment they would be carrying or wearing. It is equally important, he said, for the numerous and diverse safety organizations likely to be involved in such responses to know how to work together. Also, emergency workers need to know how to rescue and treat people in an environment that is or may be contaminated.

“Our philosophy,” Richmond said, “is that if you build an EMS system that works well every day, then it will also work well when something much more unexpected happens. But,” he quickly added, “we also have to give our providers some special tools, skills, and knowledge to deal with the unexpected.”

Adam McLaughlin is with the Port Authority of NY & NJ, and is the Preparedness Manager of Training and Exercises, Operations & Emergency Management, where he develops and implements agency-wide emergency response and recovery plans, business continuity plans, and training and exercise programs. He designs and facilitates emergency response drills/exercises for agency responders, state and federal partners, and senior Port Authority executives.

WHERE THE MISSION IS TO SECURE OUR NATION

See the future of government security **ONLY** at GovSec/U.S. Law 2010!

Join your colleagues and others in the domestic preparedness community for the leading Symposium, Expo and Educational event of the year—all in one!

DOMESTIC DEFENSE SYMPOSIUM **NEW!**

Attend targeted tracks that provide insight into the topics most relevant to your agency or business, including:

- The Domestic Defense Priorities of the Obama Administration
- Coordination Between the Military and First Responders
- The Role of the U.S. Military in Capturing Terrorism Suspects on American Soil
- Coping With Less: How States are Dealing with Reduced National Guard Presence Due to Military Commitments in Iraq and Afghanistan
- Intel Gathering and Sharing for Domestic Defense

FREE* EXPO

Experience the newest systems, tools and technologies preventing future incidents, preparing for and responding to all hazards and disasters, and ensuring the public safety.

Featured areas on the show floor:

- Focus on Digital Forensics **NEW!**
- Cybersecurity Pavilion **NEW!**

PLUS see, touch, and learn first hand about hundreds of security products and services focused on:

- Access Control, Intrusion Detection, Perimeter Security, Surveillance
- Communications, Wireless & Internet
- Disaster Preparedness & Recovery
- Intelligence Analysis & Homeland Security Software
- Threat Detection Systems

OFFICIAL PUBLICATIONS



PRODUCED BY



ADDITIONAL EDUCATION FREE* FOR ALL WHO ATTEND

Highlights include:

- Homeland Security Finance Forum **NEW!**
- International Initiatives on Cybersecurity **NEW!**
- Whats Next in DNSSEC **NEW!**
- Theater presentations featuring the latest technology products

Thousands of your colleagues are already attending. Don't miss your chance, register today for only comprehensive government security expo and conference of the year!

*The GovSec/U.S. Law Expo and Education is FREE for all government, government contractors, and military; and only \$50 for others to attend.

Interested in exhibiting at GovSec/U.S. Law 2010?
Email exhibit.govsec@1105govinfo.com.

**UNCOVER THE CRITICAL INFORMATION
YOU NEED TO COMPLETE YOUR MISSION**

**PLEASE USE PRIORITY CODE
NW1S12 WHEN REGISTERING**

REGISTER TODAY!

FOR FULL EVENT DETAILS AND TO REGISTER:

www.govsecinfo.com

Connect with GovSec/U.S. Law on

facebook

govloop

LinkedIn

twitter

YouTube