domestic preparedness .com

DomPrep Journal

US Annual $100 Volume 8 Issue 12, December 2012

The Next Big Thing

Phoenix

Lightweight, low burden CBRN protection

Phoenix

Lightweight CBRN protection suit

The Phoenix CBRN Protection Suit combines the most versatile operational CBRN protection technology along with functionality for the military and civil security services around the world

http://frontline.remploy.co.uk

USA Tel: 001 540 604 4478
USA Email: frontline@remploy.com

Remploy
Putting ability first

Frontline

The Phoenix provides CBRN protection in a high threat/low hazard environment where a wide range of challenges are present

Lightweight and highly breathable, the Phoenix is an effective emergency CBRN protective solution that allows both commanders and users to maximise their full operational capabilities and functions, even in the most challenging environments

- 10 year shelf life
- Up to 20 times laundering
- 30% lighter than current systems
- Greater breathability and lower thermal burden
- Compatible with a range of respirators
- Inherently fire retardant
- Provides both emergency CBRN and general purpose functionality

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
Director of Marketing & Sales
scollins@domprep.com

Catherine Feinman
Associate Editor
cfeinman@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

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

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 Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher.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

IMR GROUP

Editor's Notes

By James D. Hessman

DomPrep's annual forecast issue is entitled "The Next Big Thing" and features eleven distinguished authors, all of them recognized experts in their various fields of endeavor. James Lee Witt, for example, a true Washington insider, points out that the looming fiscal cliff so much in the news these days may well result in additional budget reductions for the U.S. Department of Homeland Security, the U.S. Department of Health & Human Services, and other homeland-defense agencies. For that reason, he calls for closer, more inclusive, and continuing cooperation between and among local and state as well as federal and private-sector organizations and agencies.

Craig Crume also sounds a note of optimism related to recent and prospective improvements in equipment, medicines, and communications, but points out the many problems created by not including on-scene responders in the advance planning phases of new policies and procedures. Marko Bourne discusses the major improvements likely to be derived from the emergence of "cloud" computing and its relevance to the nation's first-responder communities.

Timothy L. Tinker also voices optimism, based on the already proven use of social media to improve and expand the communications capabilities needed to deal, quickly and effectively, with sudden emergencies, including both natural and manmade disasters of all types. Daniel J. Abdun-Nabi promises additional improvements, particularly in the development and use of new medicines and medical countermeasures, thanks in large part to the establishment of three new "innovation" centers – in Texas, North Carolina, and Maryland – for the advanced development and manufacture of those medicines and countermeasures. And Christopher Wrenn points out several ways in which chemical warfare agent detectors can also be used to cope with other types of dangerous incidents and events.

So there is reason for optimism – several reasons for pessimism as well. Scott Jackson, for example, discusses resilience, the organizational, physical, and procedural factors involved, and a broad spectrum of planning and operational principles that must be observed in building resilience; each of those principles, though, he also points out, is accompanied by one or more potential liabilities. Joseph Cahill focuses special attention on the lifesaving medical care provided by first responders at the scene of a major incident, and notes that numerous legal and financial factors must be taken into consideration before deciding whether "basic," "advanced," or "extraordinary" medical care should be used.

J. Michael Barrett is both optimistic and pessimistic, and adds a bit of historical perspective. The modernization of the nation's power grid, he points out, has rightly been hailed by experts as perhaps the "greatest engineering achievement" of the 20th century. That same grid, though, is today much older, decrepit, subject to sudden and repeated failures, very costly to maintain and even more costly to repair, and now likely to become the "most vulnerable infrastructure" of the 21st century.

Glen Rudner shifts to a global and even darker possibility – namely, that the current civil war in Syria could be quickly followed by the transfer, to other nations or even terrorist groups, of chemical weapons that could and very possibly would be used against the cities and populations of various Free World nations.

Rounding out the issue is an interview conducted by Aaron Poynton with the Honorable Paul McHale, who addresses his concerns about the current state of homeland defense and disaster response. Although the future holds many uncertainties, there are ways in which the preparedness, response, and recovery communities can make a difference, raise the bar, and improve the outcome.

About the Cover: DomPrep's annual "Forecast" issue sheds some much-needed light on the major homeland security issues facing first responders and decision makers in the coming year. Prediction: Major new and difficult challenges – largely offset by better long-range planning, improved technology, and a more inclusive spirit of cooperation at all levels of government. (iStock photo)

Implementing the National Health Security Strategy

A Five-Part White Paper Series by

RADM Craig Vanderwagen, M.D.

Founding Assistant Secretary for Preparedness and Response,
U.S. Public Health Service - Retired

The strategic goal of delivering needed supplies and people to populations during disaster events, natural or manmade, is to save lives, reduce the burden of suffering and to speed recovery to a new normal after an event. This white paper series explores the role and requirements for a system of information management in directing and utilizing medical and public health assets in preparation of and responding to events.

White Papers Now Available for Download:

Part 1: The Role of Logistics in Public Health Practice
Part 2: The Role of Patient Tracking in Public Health Practice
Part 3: The Public Health Challenge in Mass Evacuation & Shelter Care
Part 4: Event Management: Visibility in the Fog of Response
Part 5: A National Strategy: It Is Time For Action

Watch Dr. Vanderwagen in a video preview of each white paper at **upp.com/vanderwagen**

From August 2006 until July 2009, **Dr. Vanderwagen** was the founding Assistant Secretary for Preparedness and Response (ASPR), U.S. Department of Health and Human Services.

White Paper Series Underwritten by:

Upp Technology, Inc.
800.777.6092 | upp@upp.com

innovative technology solutions

Download the White Papers today at **upp.com/vanderwagen** or scan this code.

Superstorm Amplifies Need for Power Grid Modernization

By J. Michael Barrett, CIP-R

As several million Americans continue to struggle with the devastation wrought by Superstorm Sandy, it is worth asking how the nation can better prepare to weather future natural and manmade disasters. This is particularly important in considering one of the storm's most important impacts – namely, its near-total destruction of the electrical power grid and associated infrastructure in the states hit hardest by the storm (and the nor'easter that followed). The national electrical grid has been described by the National Academy of Engineering as the greatest engineering achievement of the 20th century. Another disaster similar to Superstorm Sandy, however, might make it the most vulnerable infrastructure weakness of the 21st century.

The electrical power grid was also the foundation, for 100 years, of the most profound and dynamic economic growth the world has ever seen, providing a reliable source of energy for America's industrialization and modernization. Access to dependable and affordable electricity, of course, remains critical to continued productivity and prosperity of any modern economy so heavily reliant on digital devices and ever-flowing data streams. However, the increasing frequency and severity of natural disasters and weather events in recent years, the potential impact of cyber or terrorist attacks, and the constantly growing energy needs of a still growing population all require a more resilient and reliable electrical grid that can satisfy the national demand and mitigate the risks posed by additional systemic failures.

Assessing Risks & Setting Goals

Here it is important to note that most risk estimates are based both on the likelihood of an event and its potential severity – which means that frequent but minor events such as thunderstorms trigger different policies and safeguards than are required to cope with much more serious events including terrorist attacks. However, previous calculations of the risks to the U.S. electrical grid are proving to be both inaccurate and obsolete. For instance, storms such as Hurricane Katrina and Superstorm Sandy were once considered extremely rare events and for that reason it was not believed, by the general public as well as government officials, to be cost effective to invest in large-scale preventive measures.

In recent years, though, that view is changing, and there is general (but not universal) agreement that both the frequency and the severity of destructive weather events are increasing. If that view is correct, it means that earlier cost-benefit analyses are dangerously out of date. In fact, a recently declassified 2007 report – entitled "Terrorism and the Electric Power Delivery System" and released in November 2012 by the National Academy of Sciences – suggests that the entire U.S. electrical grid system is now vulnerable to attacks by terrorists using little more than high-powered rifles at a few key locations. Although the

likelihood of such an event may be quite low, the severity of a well-planned attack still could be devastating with a significant loss of life caused by the power outages that would follow. In today's massively interconnected world, small and seemingly isolated events can quickly escalate into major systemic disruptions affecting large areas of the country. Such disruptions were demonstrated not only by Superstorm Sandy, but also by the massive 2003 northeast power blackout when some 50 million people lost power across the Northeast and Midwest for up to four days.

Given such examples, and the fact that even more massive disasters – terrorist attacks as well as weather events – are entirely possible, it seems clear that the policies in place to protect the nation's entire electric grid must be upgraded to become smarter, more resilient, and more reliable. To meet that ambitious goal, though, requires well-coordinated and factually based policy decisions.

Gaining Efficiencies by Updating & Standardizing

Fortunately, some of the changes needed are obvious. For example, former New York Governor George Pataki, writing in the 25 November 2012 issue of *The Wall Street Journal*, focused special attention on an emergency relief policy that exposes some of the fundamental weaknesses of the current system. Specifically, the Federal Emergency Management Agency (FEMA) provides funding to electric utility companies to replace damaged electrical components only when those funds are used to purchase components based on the same technology. In other words, the new components are often outdated and just as vulnerable to disruption as the old components when the next event occurs.

This highly inefficient policy not only hinders innovations and either slows or prevents rational upgrades but also actually encourages utilities to maintain inventories of technologically obsolete components – some of which are more than 30 years old. Moreover, and largely because the system was built piecemeal, such backward-looking policies create missed opportunities to foster standardization and interchangeable parts, which could cut costs by streamlining logistics and repair work.

One simple policy solution is to require the use of interchangeable parts and standardized designs for components that either can be replaced in whole or as separate modules serving discrete purposes. Adoption of this policy would make it easier for utility companies to maintain a sufficient stock of spare parts. Implementing such a policy also could modernize and standardize the interfaces of other material assets ranging from gaskets and valves to interoperable control systems and computers using seamlessly integrated enterprise software systems.

The efficiency gains achieved from the use of standardized and interchangeable parts would result not only by having many fewer parts in the overall inventory but also from making it easier to quickly replace a portion or all of a damaged system with equivalent "off-the-shelf" (as opposed to custom-designed) spare parts. This approach is already being used in many modern industries, but it was not a feature of the original designs used in the decentralized U.S. power grid infrastructure. As a result, there now is a great variance in the sizes, power requirements, weight, and other characteristics of numerous critical generation, transmission, and distribution parts.

Greater uniformity would facilitate more, and more cost-effective, repair solutions by eliminating the need to have fully redundant components in place that may go unused for days, months, and even years. An added benefit of shifting to a more uniform approach is that the various stockpiles of spare parts can quickly and easily be shared across regions – and across industry partners – and thus more broadly spread out the system-wide cost of buying and storing the same items. There would be an important safety and operational bonus as well – namely, in the event of a widespread power outage, utilities and emergency relief services could more quickly and efficiently make needed repairs to the system in order to restore electricity.

Tough Leadership Decisions

The choice in this area facing decision-making officials at all levels of government is clear: Do they face up to the difficult challenge ahead by capitalizing on the opportunities made possible by preventive pre-event improvements, or continue business-as-usual policies based on obsolete technology and no-longer viable policies? Disturbingly, a 2009 study on natural disasters by Professors Andrew Healy and Neil Malhotra, entitled "Citizen Competence and Government Accountability: Voter Responses to Natural Disaster Relief and Preparedness Spending," found that voters

rarely reward preventive spending on disasters, but they do highly reward post-event public expenditures. For that reason alone, it was no surprise that, in the aftermath of Superstorm Sandy, the voter-approval rating of New Jersey Governor Chris Christie reached an all-time high.

As history has shown, however, true leadership is demonstrated by doing what has to be or should be done, even if it is not widely recognized as important – regardless of the positive and/or negative political factors involved. Americans must better understand the current and future risks to the nation's electrical grid system – and the likely costs of failing to modernize it for the 21st century. It also would be helpful if the nation's leaders – again, at all levels of government – take the actions needed to protect and advance the vital interests in national and economic security by making the "greatest engineering achievement" of the last century viable again, both financially and technologically, for the next 100 years.

For additional information on:

Andrew Healy and Neil Malhotra, 2009, "Citizen Competence and Government Accountability: Voter Responses to Natural Disaster Relief and Preparedness Spending," visit http://myweb.lmu.edu/ahealy/papers/healy_prevention_070808.pdf

National Academy of Sciences, 2012, "Terrorism and the Electric Power Delivery System," visit http://www.nap.edu/catalog.php?record_id=12050

George Pataki, 2012, "In Sandy's Wake, Time to Upgrade the Power Grid," The Wall Street Journal, visit http://online.wsj.com/article/SB10001424127887324735104578119002091499238.html

---

J. Michael Barrett is the CEO of Diligent Innovations, a D.C.-based strategy and policy consulting firm, and Adjunct Fellow with the Lexington Institute. A national security expert and noted author with an extensive background in defense policy, military intelligence, and support to U.S. counter-terrorism operations, his extensive national security credentials include serving as the Director of Strategy for the White House Homeland Security Council, Intelligence Officer for the Office of the Secretary of Defense, and Senior Analyst for the Chairman of the Joint Chiefs of Staff. He is also a former Fulbright Scholar to Ankara, Turkey.

Additional contributions to this article were made by:
John Thorne is a Senior Analyst at Diligent Innovations focusing on science and technology policy for national security needs. A strategic and counterinsurgency expert with an extensive background in national security and stability operations, he formerly served with the U.S. Army in Kandahar, Afghanistan, and as a Social Scientist with a Human Terrain Team at Forward Operating Base Spin Boldak. He holds an MA in International Relations from the Johns Hopkins School of Advanced International Studies.

Jeff Harner is a Senior Analyst at Diligent Innovations supporting the Office of the Secretary of Defense. An experienced business and economic analyst with an extensive background in finance, national security, and economics, he formerly served as a Department of Army Civilian in Wardak and Logar provinces, Afghanistan, and as a Social Scientist with the Human Terrain Team. He holds an MA in International Relations from the Johns Hopkins School of Advanced International Studies.

Emergency Management in 2013

By James Lee Witt, Emergency Management

Emergency management can be one of the most challenging but at the same time exceptionally rewarding fields of human endeavor. As unexpected crises and natural disasters become more numerous and more intense, the need for a strong, coordinated, and well-resourced emergency management infrastructure in place is absolutely imperative.

In the past decade, fortunately, several new degree programs have emerged to educate the next generation of emergency management leaders. As a result, today's disaster management teams – at all levels of government and in the private sector as well – are highly trained and prepared professionals who not only play an increasingly important role in the short-term responses to disasters of all types, but also in the long-term and complex rebuilding of entire communities.

Budget Cuts & Planning Woes

Recent economic woes and the potential fiscal cliff now much in the news are forcing federal, state, and local governments to make some extremely difficult choices in their funding priorities. In 2013, newly elected and re-elected U.S. officials will undoubtedly be considering new fiscal reductions in the infrastructure of emergency management and other key areas that support the plans of most agencies, at all levels of government, in their efforts to balance their budgets.

At the federal level, even after a reduction in the Department of Homeland Security (DHS) budget for fiscal year 2012, many experts are already predicting a further reduction for fiscal year 2013 – and, quite possibly, a smaller role for the department's Federal Emergency Management Agency (FEMA), particularly if DHS reshuffles its priorities. Budget cuts at DHS (and FEMA) would undoubtedly lead to a reduced level of support for state and local homeland security and emergency management agencies, thus forcing all of those agencies to take a fresh look at how to effectively support their still critical functions.

Obviously, emergency managers should work aggressively to protect emergency management's current high priority in public budgeting. However, they also should intelligently plan for how such work can still be done, fully and effectively, if the federal government's funding for emergency management is jeopardized.

Collaboration, Partnering & Leadership

Clearly, disaster planning, response, and long-term recovery efforts work best when the process is collaborative. As the recovery phase begins, to consider one current example still very much in the news, important lessons already have been learned from Superstorm Sandy – the most important "takeaway" at this point seems to be the key role of multi-level partnerships. A well-executed recovery, therefore, necessarily involves the federal, state, and local governments working together on an ongoing basis. The sharing of physical resources and professional staff is critical for meeting the needs of affected communities – and can also have a positive impact on public budgets that already are stretched very thin.

In addition to the "standard" partnerships between governmental entities at different levels, 2013 is likely to see more effective partnering between neighboring states. To cite but one example, it is now imperative for state leaders to develop and implement Emergency Management Assistance Compacts (EMACs), which are pre-existing legal agreements between states that allow them to share resources – usually for relatively short periods of time – if and when a disaster occurs. Working in this way with neighboring states generally results not only in lower costs, for all of the EMAC partners involved, but also the speedier delivery of assistance during the critical first few weeks of a crisis. Making the process even more attractive is the fact that the costs of mobilizing resources from other states through EMACs are an eligible expense subject to reimbursement from FEMA during and after a presidentially declared disaster.

Thorough pre-disaster planning requires leaders to identify, ahead of time, the critical resource needs and staffing gaps that they may have to address in future times of crisis, and to develop the capabilities to acquire that assistance. Some municipalities, and at least a few state governments, understandably do not already

possess sufficient resources to respond to a large-scale disaster and/or to manage a long-term recovery – and for that reason will have to acquire outside emergency management resources to fill the gap.

For that reason, it is often advisable for states to have in place a detailed "pre-event" contract that can be quickly and fully activated in times of disaster. Such just-in-case planning can provide additional staffing capacity in many areas, including but not limited to: the function of Emergency Operations Centers; the assistance needed to understand and apply for federal recovery programs; the rapid deployment and use of robust public assistance and small business continuity programs; and even the removal of debris left behind in the wake of a disaster.

Granting Assistance to States: Lessons From Katrina & Sandy

Emergency management agencies share the ability: (a) to supplement the short-term immediate response to a disaster; and (b) to receive assistance in building their own capabilities in areas of disaster operations, particularly those in which they currently lack the expertise. Doing so is now all but mandatory, in fact, for jurisdictions that may be forced to cope with large-scale disasters such as Hurricane Katrina and Superstorm Sandy. To guard against that contingency, the governors of every state should begin to: (a) write, sign, and promulgate standby contracts; (b) develop and sign EMACs; and (c) build as much surge capacity as possible to cope with even the smallest of disasters on short or no notice. Fortunately, as elected decision makers wrestle with 2013 budgets, this avenue to recovery and resilience is one likely to be considered more often, and more carefully, than ever before.

One key goal in preparedness planning for the nation's elected leaders, at all levels of government in 2013, will undoubtedly be to find (or create) substantial cost savings without adversely affecting the ability of DHS, FEMA, and other agencies to carry out their critical missions. Accordingly, 2013 may bring a much-needed rethinking of FEMA's grant programs to states by restructuring these programs so they are administered by the states. This would decrease FEMA's overhead significantly by reducing its number of full-time, contract, and reservist staff. Shifting administration of the grant programs to the states also could help strengthen preparedness across the country by promoting more local leadership "on the ground" rather than far away in Washington, D.C.

Emergency management professionals already know a thing or two about responding to disasters. The United States has been fighting through its own economic disaster over the past few years, and the response and long-term recovery should be one that is efficient, well-planned, and effective. Although the nation's economic woes put immense pressure on government to tighten budgets, leaders and planners must not lose sight of the importance of emergency preparedness as it affects the health and safety of the nation. A strong and continuing commitment to emergency preparedness will in any case significantly reduce the adverse consequences of future disasters and help maintain the strong communities needed both before and after disasters strike.

James Lee Witt is Chairman and Founder of Witt Associates, a public-safety and crisis-management consulting firm based in Washington, D.C., that provides disaster-recovery and mitigation-management services to numerous state and local governments, educational institutions, private-sector businesses and corporations, and the international community. As a former FEMA Director, and the first to be elevated to cabinet status, he played a key oversight and decision-making role in the U.S. responses to more than 350 major disasters and is widely regarded for promoting mitigation and disaster risk reduction efforts. He is a special advisor to the State of Louisiana to help the long-term recovery from Hurricane Katrina, and is currently helping the State of New Jersey recover from Superstorm Sandy.

From Risk to Resilience: A Social Enterprise Model

By Timothy L. Tinker, Viewpoint

Since Hurricane Katrina, extreme natural and man-made events have strongly influenced how the federal government – the Federal Emergency Management Agency (FEMA) in particular – has responded to major and unusually complex disasters and threats. What has emerged in terms of lessons learned is the recognition that simply responding is not enough. Public expectations about what should happen, and when, have evolved at such a pace and level of sophistication that adaptability, agility, and community engagement have become central requirements in FEMA's response policies, protocols, and lexicon.

A number of important forces and trends are already shaping how FEMA effectively communicates and engages key stakeholders by, among other actions:

- Engaging audiences driven by a 24-hour news cycle and a social media environment in which FEMA's performance is evaluated constantly and instantaneously;
- Understanding the added complexity associated with the expansion of human-constructed environments and their interactions with the natural environment;
- Optimizing the agency's own social capital by building and sustaining strong working relationships prior to the start of various emergencies and disasters;
- Adopting enterprise-wide methods for decentralizing and democratizing data – and making policy real by building networks based on trust, reciprocity, and inclusiveness;
- Integrating new and proven leadership skills;
- Understanding, valuing, and embracing the full potential of the "whole community" concept; and
- Harnessing the power of resiliency as being more than just an improved operational response with an enhanced state of mind, belief in the mission, high level of confidence, and solid leadership.

The risk (or benefit) of anticipating, preparing, and responding to any of these trends can be significant. For example, in its response to Superstorm Sandy and its aftermath, FEMA's situational awareness mindset significantly improved the agency's capability to: (a) anticipate real and potential cascading or unexpected events that could lead to increased operational or communication failures or missteps; (b) leverage interdependencies across agencies; and (c) monitor and track the influence of the social media in shaping how audiences access, share, and act on information.

The Building Blocks of A True Social Enterprise

Social capital plays a critical role in building resilient communities and is rooted in a deep level of community trust and connectedness that fosters respect, cooperation, and collective action. In order to fully harness the power of social capital, the next logical step for FEMA is to adopt and integrate a forward-looking "Social Enterprise" approach in its outreach and engagement efforts. The principal building blocks of that approach would be social motivation and social marketing as well as use of social media, various social measures, and social models. Following is a brief summary of how each of those terms would fit into the overall social enterprise:

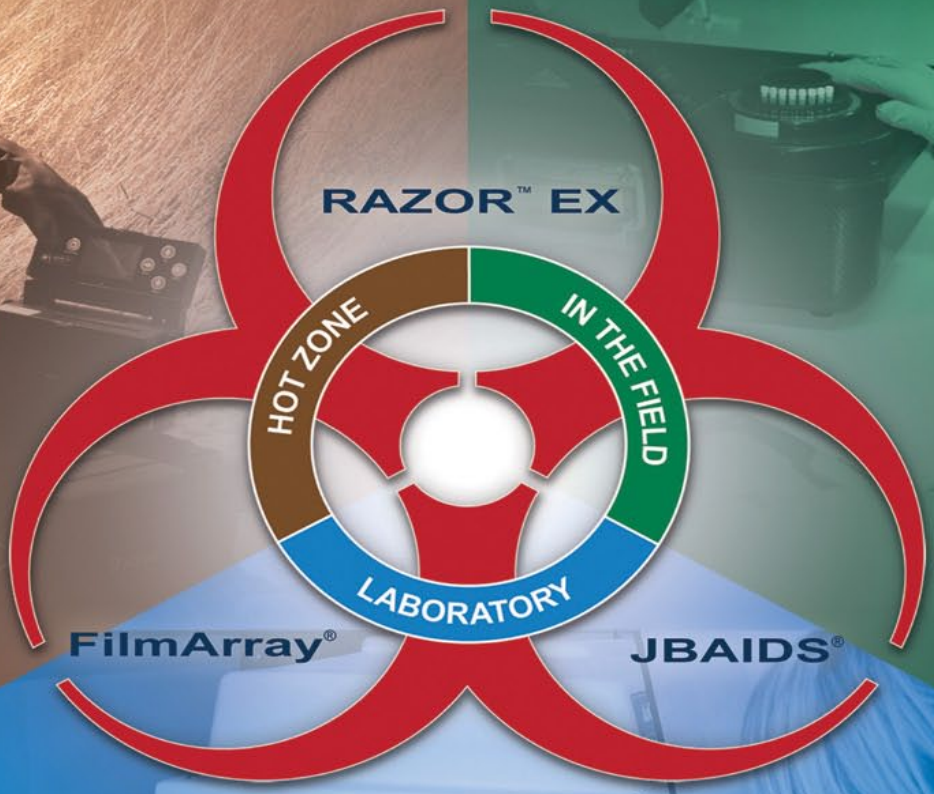
Social motivation – Communicating the "why" of mitigation and resilience: At the heart of nearly three decades of risk-science research and practice are well established social, cognitive, and behavioral theories and principles. That research would assist in many ways in identifying and informing the conditions, factors, and/or events needed if an individual or group is to be persuaded or dissuaded. For individuals, FEMA's communications should help answer fundamental questions about how various actions – or, sometimes, the lack of action – can affect both the financial and human costs of a disaster as well as the ability to deal with uncertainties and consequences. At the community level, understanding the perceptions that motivate action or inaction can help inform FEMA's own broader communications strategy.

Social marketing – Converting social awareness to social capital: Social marketing augments FEMA's current public communication strategies primarily through the

BioSurveillance

Flexible, Accurate, Proven Ready

BioFire Diagnostics delivers a fully integrated suite of Biological Agent Identification Systems. Since 1998 we have fielded BioSurveillance products that span the range of operations from the lab to the field, clinical diagnostics to environmental surveillance.



Idaho Technology is now

BIOFIRE DIAGNOSTICS, INC.

Discover the system for your mission.

WWW.BIO-SURVEILLANCE.COM

application of commercial marketing principles. The effective use of social marketing enhances social awareness, which in turn leads to optimizing social capital. The social marketing model has been used successfully over the past 30 years to create and promote social and behavior changes in such well known public awareness campaigns as the use of seatbelts and the application of sunscreen lotions. By applying social marketing to risk mitigation, FEMA can use what are called the "8 Ps" to reach target audiences and change behavior: Price (e.g., monetary and non-monetary costs); Product (e.g., information and materials); Place (e.g., communications channels); Promotion (e.g., techniques); Public (e.g., external/internal groups with a vested interest); Partnership (e.g., with credible like-minded associations and agencies); Policy (e.g., procedures and guidelines); and Purse Strings (e.g., grants, donations, gifts).

Social media – Sharing the right message with the right people at the right time: Effective media interaction and the use of social media tools and techniques help provide FEMA's key stakeholders with timely, accurate, and consistent risk information. When optimally combined and deployed, the offline as well as online media can and should be integral to facilitating information exchanges aimed at promoting actions that include but are not limited to the following: building, maintaining, and/or restoring trust; improving consumer and media knowledge and understanding; guiding appropriate and protective attitudes, decisions, and actions; and encouraging collaboration and cooperation. All of these goals can be achieved through proactively engaging communities about risks that they themselves can control and/or by dissuading individual citizens, or groups, from actions and/or behaviors that increase risk.

Social measures – Harnessing strategic tools and techniques: By employing best practices, FEMA will ensure that its strategy aligns with its operational as well as communication objectives. New visualization and social media techniques help communicate the complex nature of risk and employ rigorous, reproducible, and repeatable methodologies and tools – and, by doing so, will improve situational awareness, real-time analytics, decision making, public and partner engagement, and both operations and information management.

Social models – Building and sustaining resilient communities: FEMA's ongoing public outreach efforts have allowed a number of communities to better prepare for and respond to natural disasters. Applying social marketing and whole community models will help the agency further increase the community adoption of risk-prevention actions. In the short as well as long term, these measurable increases and improvements in actions taken will help FEMA better meet the U.S. Department of Homeland Security's overall stated objective to "strengthen nationwide preparedness and mitigation against natural disasters."

Timothy (Tim) Tinker, DrPH, a nationally recognized expert in risk and crisis communications, is a senior associate and director of Booz Allen Hamilton's Center for Risk and Crisis Communication, which provides a broad knowledge base of best practices and tactics to effectively plan for, respond to, and recover from emergencies and disasters. Before joining BAH, he was senior vice president (2001-2007) of Widmeyer Communication, where he formed a national and global network of risk and crisis communication experts to assist such major federal agencies as the U.S. Department of Defense, the U.S. Department of Agriculture, the U.S. Environmental Protection Agency, and the U.S. Centers for Disease Control and Prevention. Before entering the private sector, he had a long and distinguished government career, as chief of communications and research at the Agency for Toxic Substances and Disease Registry, a sister agency of the Centers for Disease Control and Prevention in Atlanta, GA. He received his doctorate from University of Texas Health Sciences Center.

Extraordinary Care: A Case Study for the Future

By Joseph Cahill, EMS

There is some debate over whether more care than is presently administered should be provided before a patient is transported to the emergency room of a hospital. The shifting of treatments and/or diagnoses from the hospital to the ambulance is appropriately described as "extraordinary care" (EC), primarily because such shifts exceed the "normal" Advanced Life Support (ALS) standard of care that paramedics or Basic Life Support (BLS) that EMTs (Emergency Medical Technicians) now provide.

In addition to the additional training required, there are significant other concerns that also must be considered. For example, paramedics and EMTs operate under what is called delegated practice. In effect, an agency's medical director authorizes emergency medical services (EMS) providers to practice medicine under the director's own license – and, for that reason, many state laws, local oversight requirements, and agency policies limit the scope of the medical care delegated.

Another concern among those in the medical oversight community is that each system may have variations in the models used for EMS. Thus a single county may have several volunteer agencies, private for-profit firms working under contract, and/or a full-time municipal staff as well. The rules for staff with paid training built into their full-time schedules, or with a high call volume and who therefore gain experience more quickly, must apply equally to other staff members. The latter may work on the ambulance only one or two shifts a week or even month – and often receive training on their own time and at their own expense.

Some agencies may see EC as an extra service available to their patients and therefore view it as a point of pride, but others may struggle to cover the bills while providing only baseline care – and still others may have a financial responsibility to owner groups requiring cost controls and therefore see EC as an unnecessary or unwarranted expense.

Providing extraordinary care involves additional expenses and medical as well as financial liabilities and risks. The benefits must be carefully calculated against potential costs to determine the level of care that should be provided outside the hospital setting.

Cost, Liability, Risks & Benefits

The services currently provided by paramedics across the United States usually are charged at a flat rate. Although agencies are permitted to charge more for ALS than they do for BLS, these additional charges do not extend to EC; there is no rate for ALS plus. As a result agency managers may not want to deal with the burden of the additional costs entailed in providing extraordinary care. In fact, many managers may rightly view EC as an additional liability.

Some systems have implemented EC plans and policies by applying to oversight agencies for "pilot projects" to prove the safety and efficacy of such care when provided in an EMS setting. By defining the project scope to include the entire system, regulators usually can ensure that the EC is implemented only by an agency capable of filling the added requirements both safely and effectively. Such pilot projects, however, often raise the bar and thereby encourage other agencies to follow suit – in fact, many current treatments that are now standard originally were considered to be extraordinary care.

Most if not all EC practices are undoubtedly an additional uncompensated expense – particularly when carried out by for-profit agencies. Although unable to transfer the added expense to the patient, the cost can be built into a contract with the local jurisdiction. EC can also be included in the marketing strategy used to demonstrate both an agency's professionalism and its leadership role in the local EMS community.

As with any other liability discussion, professional advice – both medical and legal – is or should be a crucial factor that should be taken into consideration in the decision-making process. If current insurance does not cover the additional liability involved, then the additional coverage must be purchased – and that cost rolled into the operational plan spelled out for the EC.

A risk-benefit analysis also must be made – both for the agency and for the patient. Just one example is the purchase and use of a device that allows paramedics to determine the extent of an abdominal injury – and, therefore, the possible need for rapid transport to a trauma center. Such equipment is less useful in a jurisdiction – a large city, for example – where many hospitals within a short transport time are equipped to handle abdominal trauma, as opposed to a more isolated setting in which the helicopter medevac of trauma patients is required for transport to trauma centers. In the "large city" example, simply transporting *all* patients with abdominal injuries to the trauma center and spending the EC funds on something else may be a better alternative.

Implementation of an EC plan is a purely management task in that it is entirely about managing change and risk. EMS managers must therefore sometimes use a visionary style of leadership to ensure that their own agencies follow the optimum path of forward progress.

Joseph Cahill is a medicolegal investigator for the Massachusetts Office of the Chief Medical Examiner. He previously served as exercise and training coordinator for the Massachusetts Department of Public Health and as 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. Prior to that, he was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem. He also served on the faculty of the Westchester County Community College's Paramedic Program and has been a frequent guest lecturer for the U.S. Secret Service, the FDNY EMS Academy, and Montefiore Hospital.

Integrating Support for Real-Time Response Success

By Craig Crume, Viewpoint

Creating a sense of calm amid chaos, and avoiding the natural fight-or-flight response in the face of an emergency, requires confidence not only in a responder's training and tools but also in the governmental as well as private-sector support systems now available. When all of these elements work in concert, potential panic can turn into effective assuredness.

Numerous innovations in chemical, biological, radiological, nuclear, and explosive (CBRNE) equipment and instrumentation continue to simplify certain tasks and save time. Success in the field, however, depends on the responder's ability to: (a) properly deploy instruments; (b) understand their functions, limitations, and interoperability capabilities; (c) interpret results; and (d) recognize when the information is (or is not) sufficient to complete the task(s) involved. Instruments provide the data, but the operator must be able, even under duress, to provide an effective response based on that data.

The future offers a new level of integration to guide and support the most critical "component" of the emergency response community – the individual responder.

Although training definitely helps by making tools seem more intuitive – and response options more predictable – the uncertain nature of hazardous emergency incidents makes it difficult to accurately simulate such scenarios in a classroom setting. Taking control of a chaotic situation depends on the ability of responders to adapt all of their assets – training, experience, and tools – to novel situations. Invariably, responders encounter unexpected circumstances including, but not limited to, the following: equipment failures; detectors providing what seem to be contradictory results; limited availability of personnel; varying levels of expertise possessed by personnel; and unreliable communication methods. Whatever the circumstances, though, the ability of the individual responder to adapt and improvise is still an essential factor for success in many emergency situations.

Real-Time Response Support

By simplifying and streamlining response systems, operators have the ability to act more intuitively to each situation as it unfolds. Today's responders have access to an array of powerful tools – including sophisticated instruments, decision support systems, geolocation and modeling systems, learning management and training systems, resource and personnel management systems, and incident command and control systems. However, without seamless integration, those essential tools might easily become disconnected stumbling blocks. The training and support systems needed, for example, are typically one or two steps removed from the incident – and for that reason usually confined to the classroom or an equipment-repair facility.

One not always obvious factor that can change this equation is the ability to provide an experienced community of real-time, on-demand support to those in the field. Building and implementing a real-time support system probably would depend primarily on expanding and improving the integration of multiple forms of data already available from numerous sources. To accomplish this goal, of course, data and information would have to be collected quickly from multiple instruments, systems, and roles in the emergency response organization and presented to team members when and where they need it.

Similar to the many operational successes of today's global positioning systems, truly integrated support systems would quickly provide a new and operationally particularized inventory of roadmaps and workflow charts as well as a searchable and greatly expanded knowledge base. The responder would still make the final decisions but – with the equipment already available

and the new systems just over the horizon – probably would be able to do so both more quickly and with greater confidence.

Innovations in Integration

Considerable progress has been made toward a more integrated approach to training and support. Today, training is increasingly geared toward applications, targets, and categories rather than to a specific piece of equipment. Instrument operational principles are taught in the context of the responder's applications and equipment set, while "cloud-based" support systems provide help that is more specific to the responder's concept of operation. In fact, training events may contain elements of operator support, and technical support frequently takes on the role of issue-specific training.

Already, or soon to be, operational is a new generation of systems with the ability to not only provide the complete integration of training and support needed but also to translate the additional capabilities provided into the real-time operational information required at, during, and after a specific incident. Such abstract management terms as workflow, decision trees, and triage approaches will be much better understood, and troubleshooting videos on those and other topics also will be available, in real time, to on-scene responders. At the command center, meanwhile, the data and results available from a broad spectrum of different instruments and sources would be processed fully and effectively – in time to offer immediate conformational results as well as the ability to recommend next steps and fill in other data gaps.

In addition to a cloud-based multi-role support system, a support hotline staffed by CBRNE subject-matter experts would be able to offer live help to operators and repair personnel who encounter instrument problems. This service would be particularly useful in preventive maintenance and instrument repair. One example of the time and financial benefits that could be achieved: Support data collected in 2011 by KD Analytical (one of the private-sector "support systems" mentioned earlier) showed that, in certain incidents, more than 60 percent of the instrument problems that developed were resolved over the telephone – with the end-user completing the maintenance or repair. Making that support more widely available could increase equipment uptime – and also lead to significant improvements in end-user proficiency.

To briefly summarize, real-time integrated support for CBRNE responders will offer numerous benefits to the organizations and communities they serve: improved uptime and readiness; reduced cost through self-guided repair and equipment life-cycle extension; improved responder proficiency; and increased speed and efficiency during operations. In short, the future offers a new level of integration in which instrument maintenance, training, resource management, situational awareness, troubleshooting, and incident expertise all coalesce into a single real-time expert system guiding and supporting the most critical "component" of the emergency-response community – namely, the individual responder.

Craig Crume is Vice President and Co-Owner of KD Analytical Consulting Inc. He has more than 25 years of analytical experience training and supporting analytical equipment around the world and has published or presented more than 30 papers on field analysis. Since 2003, KD Analytical has provided training, instrument maintenance, and support to the CBRNE responder community through use of a web-based maintenance management system and 24-hour support center.

The Future of Data Clouds

By Marko Bourne, Cyber & IT

The U.S. Department of Homeland Security (DHS) and its Federal Emergency Management Agency (FEMA) continue to face significant challenges in the five major phases of managing emergencies and disasters: preventing, protecting against, responding to, recovering from, and mitigating events. All of which continue to evolve at a rapid pace, along with the tools of the trade. During and after almost any such event, the need for rapid and reliable information is perhaps the most critical factor involved in making effective decisions. Whether the decision window requires looking years ahead or simply analyzing an ongoing 12-hour incident command operational period, the need for reliable data continues to be the key component needed for operational success.

How to effectively use that data, though, raises a number of relevant questions, including the following: How many people might have to be evacuated? Are there enough shelters available? Is the power out – and, if so, where? Do the capabilities available match the current and possibly future needs of the city, state, or nation?

The answers to all of these questions, and many others that might be asked, require the use of accurate and timely data – as was amply demonstrated by the widespread damage and loss of life caused by Superstorm Sandy and the "nor'easter" that immediately followed. Responding to and coping with those twin disasters required the quick and effective use of a veritable flood of information, much of it changing literally minute by minute. Twitter feeds and information received from other social media sites provided a huge quantity of helpful information, as did geospatial information and power outage tracking systems. All of these combined are just a small sample of the innovative ways in which essential decision-making data is being captured, analyzed, stored, and communicated.

Intelligent Decisions & Clear Priorities – But Scarce Resources

Already resident within the federal agency community are stores of information about previous disaster events, current and past weather patterns, and flood models – as well as disaster relief spending and practical information about location of the material resources needed to support response and covert operations. The challenge facing emergency managers – at all levels of government – is to harness all of the data available from their respective "siloed" systems and build the analytical tools and capabilities needed to make quick, intelligent, and economically viable decisions.

A clear understanding of the preparedness capabilities needed and the protection capabilities allowing for critical infrastructure to be more resilient will both help lead to the use of accurate information that not only enhances real-time situational awareness but also helps determine the resource priorities for full and effective response and recovery operations. Combining the data available from an ongoing event with historical data already in the information system will help develop a better overall understanding of the current environment. That understanding should enhance the ability of decision makers to adapt to and mitigate the losses caused by ongoing and/or future threats of a similar nature.

Building and improving this type of analysis, which is ongoing across the nation's emergency-management and homeland security communities, requires more effective use of the limited financial resources that are likely to be available to federal, state, and local governments

Leveraging Visual Interfaces & Analytics: A Prime Example

Numerous federal, state, and local emergency management agencies and organizations are responsible for various disaster planning and response activities and operations. Many of them already have found that using social media provides, in most if not all emergencies, helpful and timely situational awareness to deal with biological events and other potential disasters. At the Centers for Disease Control and Prevention (in 2010-2011), it was determined that using social media provided a better and faster way to accumulate and analyze data for emergency disasters in real time. With such a solution in place, it was found that the agency could expand and improve overall

preparedness by leveraging the information flow to more accurately, and more quickly, predict the probable impact and determine the response capabilities required.

In order to reach that predetermined goal, though, the agency needed a higher level of confidence on the approaches already available to gather, analyze, and use the social media data on which it would base any operational decisions. The specific challenges faced by implementing the new solution focused on related issues such as data ingestion and normalization, the building and use of a social media vocabulary, and informational extraction capabilities.

Working with industry leaders, the agency then developed the framework needed to capture, normalize, and transform the open-source media used to characterize and forecast future disaster events in real time. The framework incorporated computational and analytical approaches into the system to help transform the "noise" accumulated from the social media into usable, and useful, information. By leveraging such esoteric algorithms as term frequency-inverse document frequency (TF-IDF), natural language processing (NLP), and predictive modeling, the agency also was able to: (a) characterize and forecast the probable numbers of injured, dead, and/or hospitalized victims resulting from a specific incident; and (b) extract other helpful information – e.g., symptoms, geographic particulars, and the demographics involved – related to specific illness incidents or events.

The solution framework built by the agency was implemented in the cloud – on virtual servers – by taking advantage of its flexible computational power and storage. The new cloud infrastructure also allowed for data capturing and use of a visualization tool, called Splunk, to mine through and analyze vast amounts of data in real time, while at the same time outputting the characterization of, and forecasting the metrics related to, various captured events.

Using Data Management To Improve Understanding

The agency's solution included the use of dashboards that characterized the emergency events captured by and reported in the social media. The visual analyses that were generated included such helpful operational tools as event extraction counts, time series counts, forecasting counts, a symptom tag cloud, and geographical isolation. The algorithms were written in a programming language called Python and incorporated into Splunk – located on Amazon Web Services (AWS).

The solution framework captured live, streaming open-source media such as Twitter and RSS (Rich Site Summary) feeds. Building upon the current best practices used in the cyber-terrorism community, the new solution enables near real-time situational awareness through a stand-alone surveillance system capable of capturing, transforming, and analyzing massive amounts of social media data. By leveraging that data and its related analytics to develop more timely and more accurate disaster characterization, the agency is able to plan and respond more effectively as well.

The future of this understanding and analysis of data is not limited, though, to the realm of social media. The federal government: (a) Is in a unique position to harness the capabilities built by the intelligence community in order to cope with weather emergencies and other disasters; and (b) Also can provide – to state and local governments – the tools they need to use the data at all levels of government to make more judicious resource decisions, understand the risks and threats involved, and both respond and recover more quickly when major weather and/or other emergency situations do develop.

Collectively, big data, the cloud, and analytics seem to be on course to be the next "Big Thing" in emergency operations and, not incidentally, to serve as one of the most cost-effective ways of building and securing a truly resilient nation.

Marko Bourne is a Principal at Booz Allen Hamilton and a DomPrep40 Advisor. He is leader of both the company's FEMA market team and its Emergency Management and Response practice, and has more than 27 years of experience in: emergency services; emergency management; policy, governmental, and legislative affairs; and public affairs. Prior to joining Booz Allen Hamilton he was FEMA's Director of Policy and Program Analysis (2006-2009) and Director of Business Development for Homeland Security (2004-2006) at Earth Tech Inc./Tyco International. He also served as acting director of the DHS National Incident Management System Integration Center and, in 2003-2004, as Deputy Director of FEMA's Preparedness Division.

Partnering to Create Reliable Medical Countermeasures Capabilities

By Daniel J. Abdun-Nabi, Viewpoint

In a public health crisis, domestic response professionals understand that saving time means saving lives. That philosophy is driving an important evolution in the U.S. government's national health security strategy. The nation now faces an increasingly diverse and unpredictable set of health threats ranging from naturally occurring infectious diseases to man-made chemical, biological, radiological, and nuclear weapons.

To prepare for this new age, the U.S. Department of Health and Human Services (HHS) has unveiled a plan to more rapidly manufacture medical countermeasures – including but not limited to vaccines, antibiotics, diagnostics, and testing equipment – in an emergency. More specifically, HHS announced in June the plans to establish three public-private centers known as Centers for Innovation in Advanced Development and Manufacturing: (a) Emergent BioSolutions in Baltimore, Maryland; (b) the Texas A&M University System in College Station, Texas; and (c) Novartis Vaccines and Diagnostics, Inc. in Holly Springs, North Carolina. The Centers are intended, among other things, to give the United States a more nimble and more flexible capacity – faster and more effectively than was ever before possible – to produce life-saving treatments in future times of a crisis.

Three public-private Centers for Innovation in Advanced Development and Manufacturing are being established to update the development and manufacturing processes used to upgrade and expand the nation's medical countermeasures capabilities.

The public-private partnership model is particularly important because it breaks down the previous stand-alone "silos" and brings together the full spectrum of experience, knowledge, and expertise needed and available from the private sector, academia, and the federal government. Under the new model, the federal government will oversee the overall landscape, thereby ensuring both a consistent approach and the proper focus on program priorities. Pharmaceutical companies offer proven capabilities in both product development and manufacturing. Smaller firms bring innovative technologies and early-stage products, and academic institutions provide both scientific experience and training expertise.

This combination of talent hopes to reduce timelines associated with securing critical medical countermeasures. Although the new collaboration directly benefits each and all of the program participants, a much more important benefit is that the nation's overall security is significantly enhanced through an expanded infrastructure, greater flexibility, improved responsiveness, and – most important of all – the earlier availability of the medical countermeasures required.

Five Critical Benefits

The Centers add the following five critical benefits to the U.S. biodefense infrastructure and public health security strategy: (a) A Faster Response to Threats; (b) A More Flexible Response to Threats; (c) Greater Investments in Workforce Development; (d) A More Consistent Focus on Innovation; and (e) A Safer and More Secure Supply of Medical Countermeasures. Following are a few additional particulars related to each of these gains.

A Faster Response to Threats: The 2009 H1N1 influenza outbreak serves as a textbook example of the importance of speed during a health crisis. Despite the tireless efforts of U.S. public health officials, it took 26 weeks to produce the initial H1N1 vaccine doses – and 38 weeks to produce enough doses to cover half of the U.S. population. As HHS Secretary Kathleen Sebelius pointed out in an August 2010 press conference shortly after the crisis, "In a business where delays cost lives, we couldn't develop and manufacture countermeasures fast enough." Such delays in developing and

manufacturing countermeasures should be much less likely under the public-private strategy. The Centers are designed, in fact, to be able to deliver initial influenza vaccine doses in just twelve weeks – roughly twice as fast as during the H1N1 crisis – and 50 million doses within four months after the identification of a specific strain, saving both time and lives.

A More Flexible Response to Threats: Health threats come in many forms. Some are completely novel "super bugs," while others re-emerge over time. Some are naturally occurring; others can be intentionally engineered by terrorists. To counter such diverse threats, the United States needs flexible manufacturing platforms that can produce more than just one countermeasure. The inclusion of pharmaceutical companies as partners in the new Centers ensures that the nation will have a much more flexible manufacturing capacity to address the array of threats on the horizon.

Greater Investments in Workforce Development: The nation's response to future threats can only be as strong as the domestic manufacturing workforce and infrastructure needed to produce the countermeasures. Saving lives, of course, is the foremost goal of the Centers, but important dividends will also be yielded for the American economy. All participating collaborators will help train the next generation of scientists needed to serve on the front lines against public health threats in numerous scientific disciplines – including but not limited to process engineering, pharmaceutical manufacturing, veterinary sciences, quality control, and regulatory matters. The Centers already have committed to strengthening their workforce development programs to train this new body of front-line personnel.

A More Consistent Focus on Innovation: The Centers also place significant emphasis on nurturing entrepreneurship. A small biotech firm developing a potentially life-saving concept might not have the requisite development expertise and manufacturing capabilities to turn new ideas into proven products. By pooling resources, though, the Centers can assist carefully selected firms with issues related to regulatory guidance, quality systems, and manufacturing expertise.

A Safer and More Secure Supply of Medical Countermeasures: The H1N1 outbreak highlighted the over-reliance of the United States on foreign sources of vaccines during times of crisis. By providing surge capacity within America's own borders, the Centers ensure that the country will have an adequate supply of domestically manufactured vaccines available to cope with future emergencies.

Thinking Big & Saving Lives

This public-private partnership-based strategy is not likely to be a passing fad. The federal government's contract with each Center, overseen by HHS, is renewable for upward of 25 years, clearly demonstrating a long-term commitment. Moreover, to complement the work of the Centers themselves, the federal government has already embarked on a closely related effort to improve how regulators test and approve medical countermeasures so that a lack of resources does not in itself stand between the American people and a proven life-saving technology.

The goal is clear. In times of future health crises, life-saving treatments cannot be delayed by outdated development and manufacturing processes. The U.S. government is "thinking big" by breaking down yesterday's silos and standing alongside both academia and the private sector to establish a smarter and faster way to provide new, improved, and greater quantities of the medical countermeasures needed to save both time and an untold number of lives during and after future health emergencies.

For additional information on:
HHS's Centers for Innovation in Advanced Development and Manufacturing, visit http://www.hhs.gov/news/press/2012pres/06/20120618a.html

Secretary Kathleen Sebelius's speech on 19 August 2010, visit http://www.hhs.gov/secretary/about/speeches/sp20100819.html

---

Daniel J. Abdun-Nabi currently serves as: Chief Executive Officer (since April 2012); President (since March 2007); and a board member (since May 2009) of Emergent BioSolutions, a global specialty pharmaceutical company headquartered in Rockville, Maryland. He previously served as: Chief Operating Officer (May 2007-March 2012); Senior Vice President Corporate Affairs and General Counsel (December 2004-April 2007); Secretary (December 2004-January 2008); and Vice President and General Counsel (May 2004-December 2004). Prior to joining the company, he served as General Counsel for IGEN International Inc., a biotechnology company, and its successor, the BioVeris Corporation (September 1999-May 2004), and as Senior Vice President, Legal Affairs, General Counsel, and Secretary of North American Vaccine Inc.

Remote **BIOHAZARD** Detection

MAB
Portable Biological Alarm Monitor

Our MAB Portable Biohazard Detection System sends an alarm immediately upon detecting any evolution to the atmospheric background. It works on a continuous real-time basis and responds in only seconds. Easily used by untrained people, it has a very low power consumption rate and is especially designed for harsh environments.

MAB has a fast start-up time and can quickly analyze atmospheric particles for chemical signatures of bacteria or toxins such as anthrax, plague, Botox, legionella, etc.

MAB has already been selected by several military forces and is used by several NBC reconnaissance vehicles, as it is not sensitive to diesel vapors and smokes. Test reports are available.

Characteristics

- Size of the box (LxWxH): 300mm x 160mm x 470mm (11.8" x 6.3" x 18.5")
- Total height: 850mm (33.5")
- Weight: 14 kg (31 lbs)
- Operating temperature: -10°C to +50°C (14°F to +122°F)
- Storage temperature: -39°C to +71°C (-38.2°F to +160°F)
- Autonomy: 10 days (refillable hydrogen cylinder included)
- Power supply: 12 - 32 V DC / 110 - 220 V AC
- Can be remote controlled
- Remote data by RS 485 outlet
- Response time: less than 1 minute
- Field tested / Report available

www.proenginusa.com

PROENGIN

140 South University Drive, Suite F, Plantation FL 33324
(954) 760-9990 • FAX (954) 760-9955 e-mail: sales@proenginusa.com

New WMD Concerns: Many Questions, But Few Answers

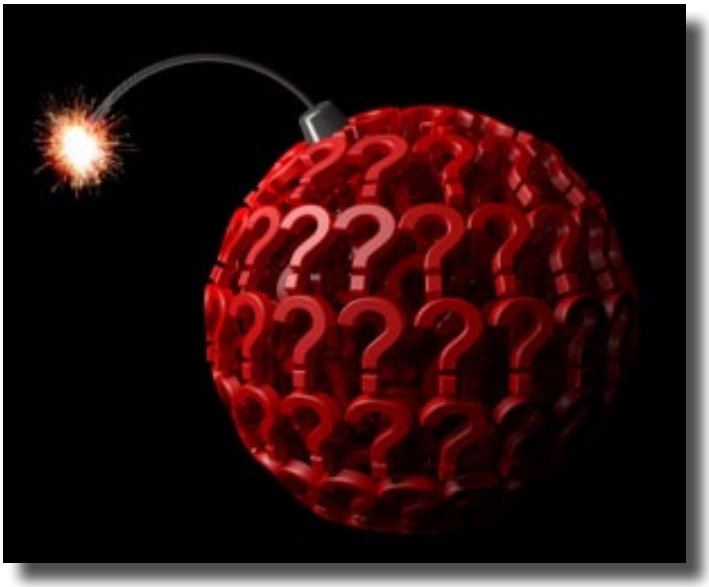
By Glen Rudner, Fire/HazMat

The U.S. first-responder community has faced a multitude of technological threats in the complex field of counter-terrorism, many of them involving chemical, biological, radiological, nuclear, and/or explosive (CBRNE) weapons. However, the threat posed by such weapons of mass destruction (WMDs) has diminished slightly in the past few years for two principal reasons: (1) Such weapons have not been used recently against the United States itself; and (2) There have been several other major issues that have seized the headlines.

The question that members of the response community must ask, therefore, is whether this downward trend will continue, or will WMD concerns begin to increase once again? The continuing violence in Syria and uncertainty about Iran's nuclear intentions suggest that the CBRNE threat may soon be back in the forefront, along with a renewed interest in the equipment and training that goes with it.

In Syria, President Bashar al-Assad is finding it increasingly difficult to maintain his authority. Like his father before him, he has stayed in power through the use of brutal violence. He and his closest associates are prominent members of the Syrian branch of the Ba'ath party; the former leader of the Iraqi branch of the Ba'ath party was Saddam Hussein. Moreover, at the end of the second Iraq war, there were reports of truck convoys from regions where Iraq was believed to have stored chemical weapons. The convoys were headed toward Syria, which is known to possess large stocks of chemical weapons. Given the long history of general chaos in that part of the world, it is important to ask what might happen to Assad's chemical weapons when he loses power, voluntarily or otherwise.

It also seems to be generally accepted that Iran is trying to build a nuclear weapon. The Iranian government has stated that it will use that nuclear weapon against Israel when the opportunity arises. Another relevant question



that is being asked, therefore, is whether the Iranians might sell any of their weapons to one or more of the fanatical terrorist groups scattered throughout that part of the world.

The Mideast, Japan & the U.S. Homeland

With those issues now front and center, numerous concerns related to the possible use of WMDs are once again moving to the forefront. Compounding the situation is the fact that many developers, manufacturers, trainers, and responders have not learned the lessons of the past, specifically the lessons made clear by two major terrorist incidents involving the use of sarin nerve agents that occurred in Japan almost 20 years ago.

In the first (1994) incident, in Matsumoto, the world saw what can happen when first responders are not trained in how to recognize the signs and symptoms of exposure to chemical weapons. Fortunately, it also seemed evident that, if there is no direct contact with the liquid itself, responders will likely survive the incident. (In fact, although there were some injuries, no responders died as a result of the sarin.)

The 1995 sarin attack on the Tokyo subway system, however, demonstrated how easy it would be for anyone possessing basic knowledge of the effects of nerve agents to accurately identify the chemical agent

involved. Although the advanced technology detection instrumentation used by the hazardous materials team misidentified the agent, a Japanese responder used common sense and observations to help identify and solve the problem.

A New Approach & Greater Responder Involvement

Two additional questions: (1) Has the responder community missed the obvious lessons learned from these incidents? (2) Are agencies, at all levels of government, equipping and properly training both individual responders and responder teams? In the United States, the subject of CBRNE response has evolved since 1995 into a top-down focus. The federal government has driven the issue via the use of significant funding – for both systems development and procurement – and better training.

Were World Wars I and II really the wars to end all wars? Perhaps they were simply a prelude to a more global threat posed by relatively small and unstable nations – and/or terrorist groups.

The highest priority has been to provide equipment to the hazardous materials teams, to purchase and distribute the best high-tech equipment available, and to give responders intensive training in the use of that equipment. However, in the rush to provide these devices and the training needed, the full integration of the end user seems to have been missed. During the development phase of much of the equipment now available, the new systems and detection devices always seem to work well in the lab – but not in the field. So two follow-on questions also must be asked: (1) Does the current approach significantly enhance the nation's overall response capabilities? (2) If not, what additional steps might be needed?

Clearly, the U.S. government has spent hundreds of millions of taxpayer dollars to improve the nation's counter-WMD response capabilities. But, another urgent question: To what effect? Strong emphasis has been placed on the development of capabilities, but individual responders usually have not been used to the fullest to help test those new capabilities – or even to help develop the new systems and equipment. Perhaps a more proactive multi-phase approach is needed to improve the development, testing, and deployment of equipment – and to provide the more effective training that the American people expect for their nation's responders.

It is important that the responders themselves be heavily involved in each phase of any new approach adopted to ensure that operational needs are driving the development, training, and deployment processes. The multi-phase approach should be the methodology used for each piece of equipment and each training program.

As a closing statement, the operational or tactical elements should drive the training required, not the reverse. If a new approach is in fact adopted, the system as a whole likely will operate more effectively and efficiently in the New Year – and for many years to come.

Glen Rudner is an independent consultant and trainer who recently retired as a Hazardous Materials Response Officer for the Virginia Department of Emergency Management. His 35 years of experience in public safety includes 12 years as a career firefighter/hazardous materials specialist for the City of Alexandria (VA) Fire Department; he also served as a volunteer emergency medical technician, firefighter, and officer and, as a subcontractor, served as a consultant and assisted in the development of many training programs for agencies such as the Federal Bureau of Investigation, the International Counter-proliferation Program, the U.S. Department of Justice's Office of Justice Programs, the U.S. Department of Homeland Security, and the Defense Threat Reduction Agency. He is now Secretary for the National Fire Protection Association Hazardous Materials Committee, a member of the International Association of Fire Chiefs' Hazardous Materials Committee, a member of the American Society of Testing and Materials, and Co-Chairman of the Ethanol Emergency Response Coalition.

Resilience Principles: The Search for Optimum Combinations

By Scott Jackson, CIP-R

Most current uses of the term "resilience" in relation to engineered systems reflect the fact that a system can return to a close approximation of its original function even after disruption by a threat. However, the resilience of a system depends on many other factors as well, including the outcome desired and the magnitude and type of threat involved. Moreover, different stakeholders may desire different outcomes in cases where total recovery is either not possible or not practical. When designing the system, therefore, the designer must consider many scenario-dependent factors – including the practicality and affordability of several potential solutions to various real and/or potential problems.

Resilience is often discussed in relation to infrastructure systems, with elements including but not limited to organizational factors (police and fire departments), physical factors (dams, bridges, warehouses, and office buildings), and procedural factors (fire protection protocols and law-enforcement requirements). Resilience applies to all three types of these elements – and to their integrated composites, including not only systems per se but also systems of systems (SoS). The latter are systems composed of two or more components, each established under different leadership and developed without the specific intent of interfacing with other systems.

Defining goals, collaborating with stakeholders, and implementing the best combination of principles helps planners and practitioners build resilience within and between their organizations and agencies, both public and private.

The various constituent systems – fire protection, law enforcement, and power distribution systems, for example – have been and are separately developed and operated, giving rise to what are known as *emergent* properties. The interactions between these systems often cause what are called cascading failures. For example, the public water supply in New York City was damaged on 9/11 by debris from the World Trade Center attacks, and that damage resulted in the flooding of the New York Stock Exchange.

By modeling the infrastructure with all of the component systems, and with all of their various inputs and outputs taken into consideration, decision makers *may* be able to anticipate and plan for infrastructural vulnerabilities that can lead to similar cascading failures in future emergencies. At the local level, the practitioner may be able to ensure that there is adequate physical separation between such individual components as electrical cables, water pipes, and communications lines. At the higher SoS level, resilience would require more planning to ensure that each node of the infrastructure has access to multiple sources of the water, electrical, and other services.

Nondeterminism: A Few Specifics

One key characteristic of resilience is its "nondeterminism," which means that its future state of possible recovery cannot be quickly or easily calculated through the use of standard mathematical algorithms. The reason for this nondeterminism is the unpredictability of both its time state – i.e., exactly when a threat will strike, as well as its magnitude and type – and its physical state, including the severity, quantity, and types of damage the system suffers. Given the uncertainties of these factors, it is extremely difficult and often impossible to know in advance how the system will respond to certain types of emergencies.

Although lacking the exact information, practitioners can nonetheless create models of certain systems with specific configurations incorporated to facilitate the modeling of various threats and scenarios. So-called Monte Carlo methods, which are based on repeated random sampling, can be used to model the effect of a statistically varied distribution of threat types and magnitudes on the system and, by doing so, develop a rough statistical approximation of the anticipated effects. The results of such simulations usually help the practitioner draw at least a few reasonable conclusions about the system's overall resilience.

Abstract Principles & Concrete Examples

A number of seemingly abstract principles may be applied to any system in any domain, but the applications of those principles require the design of specific concrete solutions that are both domain- and scenario-dependent. As suggested above, the concrete solutions implemented can be physical, organizational, or procedural in nature – and can be modeled in enough detail to make reasonably accurate predictions about their future effectiveness. The abstract principles used typically embody the essential characteristics that will be found in any concrete solution that implements the specific principles involved. For example, the principle of *physical redundancy* requires two independent and parallel branches, so that concrete solutions implementing that principle will have two independent branches.

A paper published on 19 October 2012 in the *Systems Engineering* journal included a long and comprehensive list of abstract principles, gathered from various sources. The following principles are adapted from that list:

- *Absorption:* The system is able to withstand the disruption level specified. (Example: A levee is able to withstand a 100-year-flood incident.)
- *Physical redundancy:* The system consists of at least two identical and independent branches. (Example: San Francisco is served by three water systems.)
- *Functional redundancy:* The system includes at least two functionally different branches. (Example: There are several ways – by car, train, aircraft, or boat, for example – to evacuate people from a coastal city.)
- *Layered defense:* There is no single point of failure that threatens the entire system. (Example: The Los Angeles Metrolink system now has two separate layers of defense available – positive train control and cab monitoring.)
- *Humans in the loop:* The system has enough capable people immediately available to handle unanticipated disruptions. (Example: A nuclear power plant.)
- *Reduced complexity:* The system is characterized by "minimum complexity." (Example: Micro-grids are being considered to reduce the growing complexity of current power grids.)
- *Reorganization:* The system is capable of quickly restructuring itself after a major disaster/disruption. (Example: The New York City power system was restructured following the 9/11 attacks.)
- *Repairability:* The system is capable of being repaired. (Example: The Hubble space telescope was actually repaired in orbit.)
- *Localized capacity:* Each node of the system is capable of independent operation. (Example: Hospitals typically have independent generators to provide electrical power.)
- *Loose coupling:* The system has flexibility between nodes to reduce the possibility of cascading failures. (Example: Power grids rely on human operators to reduce the possibility of cascading failures.)
- *Drift correction:* The system is able to anticipate and correct for an oncoming threat or hidden flaw. (Example: Positive train control detects oncoming trains and takes whatever actions are needed to prevent collisions.)
- *Neutral state:* The system is capable of maintaining a neutral state to deal with disruptions. (Example: A ban on "self-dispatching" would prevent first responders from entering buildings without proper authorization.)
- *Internode interaction:* The system is able to maintain cohesion through the use of effective communications, cooperation, collaboration, and command and control operations. (Example: Following the 2005 bombings in the London subway system, survivable communications systems were installed to maintain cohesion during and after future incidents.)
- *Reduce hidden interactions:* The system has no harmful interactions among its parts. (Example: A detailed review among sub-organizations reduces hidden and/or unforeseen interactions that might cause or lead to partial or total failure of the system.)

The Inherent Vulnerabilities Of Revered Principles

The 14 principles listed above each have inherent vulnerabilities – the potential for either harm or ineffectiveness – if they are not fully and effectively implemented. This is particularly true for principles relying on human involvement. Although there are two principles – absorption

and physical redundancy – for which the chance for harm is relatively low, they also possess certain vulnerabilities.

In applying the absorption principle, for example, practitioners must be sure there are: (a) no degradation of capability caused by aging or poor maintenance; (b) no latent faults – many of which can be detected only through rigorous audits and reviews; and (c) a robust system that can withstand threats over a wide variation in conditions. Similarly, the physical redundancy principle has vulnerabilities, including: (a) the possibility that, when two branches of the system are not truly independent, a failure in one branch can cause a failure in the other; (b) the likelihood that, if two software systems are identical, a hidden flaw in one system may also exist in the other; and (c) in organizational systems, the use of redundant communications systems almost certainly results in the transfer of ambiguous and/or incomplete information.

In many cases, two or three resilience principles must be invoked in the appropriate combinations. The specific "linked" principles depend on either the anticipated scenario problems or on inherent vulnerabilities of the primary principle. In many major disasters, for example, communication and other functions of the internode interaction principle may not survive the threat event. As a result, the absorption, physical redundancy, and/or functional redundancy principles may be selected to ensure the survival of the system functions.

Another example is that the reduced complexity principle almost always involves restructuring the system – which means, of course, that the reorganization principle may have to be invoked. Many principles, such as the neutral state and the internode interaction principles, almost always require human intervention, thus the human in the loop principle can be logically linked.

Resilience – Expensive & Inexpensive Alternatives

Some resilience solutions – redundancy, for example – are expensive by nature. The building of redundant aqueducts or dams, even if technologically feasible, would undoubtedly be expensive – but under certain political and/or economic circumstances, the high cost may be justifiable.

For an inexpensive or even no-cost alternative, the closest solution would be one that is merely procedural. Many of these would fall under the *internode interaction* principle. The least expensive solution would be removing impediments to cooperation among organizations and agencies. A major problem often encountered by emergency management organizations is the phenomenon of "self-dispatching" exemplified by the unauthorized entry of responders (or other persons) into a burning building. This was a problem at both the World Trade Center and the Pentagon on 9/11. Solutions to this problem would be procedural with a very low cost.

High-cost items become worth the price when the adverse consequences projected exceed the cost. As mentioned earlier, San Francisco built a triple-redundant water system after the 1906 earthquake. In some cases, it may be possible to perform a lifecycle cost analysis that includes the cost of the resilience enhancement actions, and then to balance that against the probable cost that would be expected if those actions were not implemented.

The challenge, of course, is that, although the cost of certain preventive actions can be determined, the cost that would have been incurred had the preventive action not been taken is necessarily indeterminate (because not all of the likely, as opposed to possible, costs can be accurately determined). Only statistical methods could be used to assist the decisions. Hence, the issue of cost is sometimes easy, sometimes difficult, and sometimes irresolvable.

Scott Jackson is a lecturer in the Systems Architecting and Engineering program of the University of Southern California (USC) and the author of Architecting Resilient Systems: Accident Avoidance and Survival and Recovery from Disruptions (published in 2010 by John Wiley & Sons, Hoboken, N.J.). He also: (a) is a fellow of the International Council on Systems Engineering (INCOSE) and chair of the INCOSE Resilient Systems Working Group; and (b) represents both INCOSE and USC on The Infrastructure Security Partnership (TISP). Jackson holds an MS in Engineering from the University of California in Los Angeles and is a Ph.D. candidate at the University of South Australia.

Significant contributions to this article were made by:

Timothy L.J. Ferris, who holds a Ph.D. from the University of South Australia – where, as Associate Director Teaching and Learning in the Defence and Systems Institute, he has responsibility for all of the Institute's teaching programs. Dr. Ferris also is supported by the International Council on Systems Engineering (INCOSE) as lead author in the Curriculum for Systems Engineering (BKCASE) Project and is the INCOSE Associate Director for Academic Research. He oversees research in the resilience of engineered systems and, with Scott Jackson, is a peer-reviewed author on that subject.

Additional Uses for Chemical Warfare Agent Detectors

By Christopher Wrenn, Viewpoint

In the United States, Type I hazardous material (hazmat) response teams – ranked (in California's 2009 Firescope list) as the highest level of hazmat team – are required to carry Chemical Warfare Agent (CWA) detectors to guard them against the possibility of a terrorist attack. However, since being fielded in quantity after the 1995 Sarin gas attack on Tokyo's subway system and the 9/11 terrorist attacks against the United States, there have been almost no instances in which they have been used to investigate actual CWA incidents in the United States itself.

Largely for that reason, neither the CWA detectors nor the first responder skill sets required to use them have received much attention. However, some CWA detectors can in fact be used for a number of other challenges that have been encountered by the nation's first responder community. For example, by addressing toxic industrial chemical (TIC) challenges outside their traditional CWA detection role, first responders can maintain greater readiness in these detectors for use in rare WMD (weapons of mass destruction) incidents and receive higher value from their detectors during routine hazmat responses.

First responders are receiving much needed training on rarely used equipment by expanding the use of chemical warfare agent detectors to missions above and beyond their usual hazardous materials calls.

Perhaps the most difficult challenge in gas/vapor detection incidents is pinpointing the source of the chemical agent used. One of the leading instruments used for "sniffing" such agents is the Photoionization Detector (PID). Most responder teams use 10.6eV lamps in their PIDs and, for that reason, will *not* detect a number of chemicals – e.g., chlorine, methylene chloride, and formaldehyde – with ionization potentials higher than 10.6 eV. Complicating the problem is the fact that PID lamps with higher ionization potential usually are not reliable enough for field use.

Real-Life Examples: Chlorine Odors & Chemical Smells

Fortunately, one Ion Mobility Spectroscopy (IMS) and multi-sensor orthogonal sensing technology has the ability to sniff for a broader range of chemicals by using a suite of sensors to "see" many of the chemicals that are not detected by the PIDs. Following are two "real-life" examples of how using this technology has allowed first responders both to see and to repair a leak when other technologies have failed:

Example 1: A fire department hazmat team received a call involving what was believed to be a chlorine odor in a local residence. The homeowner and his wife had noticed a haze in the kitchen and smelled what seemed to them to be chlorine. The hazmat team dispatched a two-man reconnaissance unit equipped with chlorine meters, pH paper, and a PID. After inspecting the residence and seeing no change in the readings, a second unit – equipped with a CWA detector that had been set to the sniffing mode – was deployed, and registered additional readings that spiked at a higher level in the kitchen. A quick check, carried out without using SCBA (self-contained breathing apparatus) gear, revealed what seemed to be a burnt electrical odor. On closer inspection the responders discovered the real source of the smell – namely, the compressor motor on the refrigerator-freezer unit in the kitchen. The homeowner had mistakenly believed that the acrid smell of burning electrical components was actually chlorine. Although the initial search took about 90 minutes, the responder team equipped with a CWA detector was able to identify the real source of the smell in only about five minutes.

Example 2: Occupants of a house reported what seemed to be a "chemical" smell. A hazmat responder entered the house carrying a five-gas monitor (including the

following sensors: O2, LEL, CO, H2S, and PID), but not wearing SCBA gear. Finding nothing apparently dangerous on the first floor, he cracked the door to the basement, sniffed the air at the top of the stairs, and saw no response on his meter. However, after taking only a few steps into the basement, he encountered an odor that, in his words, "knocked me down." A second responder – wearing SCBA gear and using a CWA detector set to the sniffing mode – located the smell in only a few minutes. It was coming from the trash, where the homeowner had disposed of the contents of a medicine cabinet. Upon further investigation, responders determined that some of the containers in the cabinet had broken, their contents had mixed, and a noxious smell was produced.

Using CWA Detectors for TIC Detection & "Routine" HazMat

CWA detectors are designed to classify different types of CWAs, but they also can be used to classify, and in some limited cases even identify, certain relatively common TICs. One example of using a CWA detector for incidents involving TICs involved a major ammonia leak at an ice plant.

Regional as well as state hazmat teams responded, using their PIDs primarily to find the ammonia leaks and assess the exposure levels before making important decisions concerning the type of personal protective equipment (PPE) required. After sealing off the leak, the PIDs continued to read high levels of "something" else that could not immediately be identified, so the responders initially thought that perhaps there was another type of chemical leaking.

However, by using a CWA detector to find areas of higher concentration and checking those findings in

a "TIC-Confirm" library, the responders determined that the high concentrations detected were actually ammonia diffusion caused by the large amounts of ice stored on the site. After the original leak was sealed, the ammonia diffused out of the ice and the CWA detector was then able to both locate and identify the precise source.

Organophosphates & Interior Ventilation

Organophosphate CWAs are chemically similar to some insecticides and, for that reason, many organophosphate pesticides may be classified in a CWA library as a "nerve" alarm. Following is yet another example of how CWA detection capabilities can be effectively used in a routine detection scenario.

A hazmat team responded to a call where the occupants of a house reported getting sick. Using their CWA detector, the team members found higher concentrations of a chemical around the perimeter of the floor, where a consistent nerve alarm occurred when the detector sniffed the areas of higher concentration. By using the CWA library and through discussions with the homeowner, responders found that the house had been treated with insecticides to counter a recent insect infestation. With the source identified, the hazmat team helped ventilate the structure and left only after additional sniffer levels indicated that the interior levels were similar to the outdoor background levels.

Although there seems to be little reason to use a CWA detector in daily first responder operations, it seems obvious that, by expanding their capabilities to encompass TIC detection, the detectors can quickly become very useful tools that first responders can rely on during their other operations. Moreover, becoming well versed in using CWA detectors on a routine basis also helps responders to be more comfortable by using them even in the unlikely possibility of a CWA-based WMD attack. In addition, many responders have found that the routine use of CWA detectors can be helpful in other incidents and events, including an indoor "air-quality" call (after application of a pesticide, perhaps).

For additional information on the above or similar incidents, click on:

Firescope California, 2009, "Firescope Standardized Hazardous Materials Equipment List," visit http://www.firescope.org/ics-hazmat/pos-manuals/haz-equiplist.pdf

The following Environics white papers:

"Are you missing something?," visit http://www.environicsusa.com/images/stories/whitepapers/sn-006are-you-missing-something2012-05-08.pdf

"'Off-label' uses of the CWA library in a ChemPro100," visit http://www.environicsusa.com/images/stories/whitepapers/sn-007off-label-uses-of-cwa-detectors2012-05-08.pdf

"Is There Something Out There?," visit http://www.environicsusa.com/images/stories/whitepapers/ap-105-is-there-something-out-there.pdf

---

Christopher Wrenn is the senior director of sales and marketing for Environics USA, a provider of sophisticated gas and vapor detection solutions for the military, first responder, and safety markets. He previously served as a key member of the RAE Systems team, and has been a featured speaker at more than 100 international conferences. He also has written numerous articles, papers, and book chapters on the use of gas detection in hazmat and industrial safety applications.

An Interview With The Honorable Paul McHale

By Aaron Sean Poynton, Interviews

The *DomPrep Journal's* Aaron Sean Poynton recently spoke to Paul McHale, the first Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (2003-2009), and former U.S. Congressman (1993-1999) serving on the House Armed Services Committee, about the Pentagon's role in securing the homeland.

Aaron Sean Poynton: *Mr. Secretary, the position of Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs is relatively new within the Department of Defense [DOD], created by the National Defense Authorization Act for Fiscal Year 2003 in response to the 9/11 attacks. What are the primary roles and responsibilities of this office? What is the difference between Homeland Defense and Homeland Security?*

Paul McHale: When Congress created the Office of Assistant Secretary of Defense for Homeland Defense, the responsibilities were envisioned in two categories: homeland defense and defense support of civil authorities (DSCA), often referred to as "civil support." Homeland defense is the war fighting defense of the U.S. homeland. By contrast, civil support describes the role DOD plays when assisting civilian authorities, most often during a response to a catastrophic event within U.S. borders, either a terrorist attack or a catastrophic natural disaster.

> *To be secure for decades to come, it is essential that the United States simultaneously strengthen its defense and response capabilities.*

The legal authorities and responsibilities related to homeland defense are derived from the Constitution under Article II, specifically the powers of the president in his role as commander in chief. In that regard, the constitutional basis for homeland defense is essentially the same constitutional authority that empowers, when necessary, war-fighting activities anywhere in the world.

Defense support of civil authorities, or civil support, is statutorily based. The legal authority to use DOD resources, both people and equipment, in support of civilian authorities is derived principally from the Stafford Act (1988), the Economy Act (1933), and other statutory provisions relating to emergency response activities. When a catastrophic event occurs in the United States, under the Homeland Security Act (2002), the lead federal agency for response is normally DHS [Department of Homeland Security], acting through FEMA [Federal Emergency Management Agency]. However, DOD's resources can be used to provide substantial assistance to FEMA. DOD has conducted such activities in a civil support role for many decades – for example, following Hurricane Katrina in 2005 and in response to many other natural disasters when civilian authorities have been overwhelmed.

Homeland defense is the war-fighting protection of the United States (DOD), whereas homeland security (DHS) is principally related to civilian law enforcement. Their common purpose is to achieve security and public safety for the American people; but rather than relying on the war-fighting capabilities of DOD, homeland security relies upon law enforcement authorities to identify, interdict, arrest, and defeat those who wish to harm our nation. Bottom line, DOD conducts homeland defense activities, while DHS and interagency partners conduct homeland security and related law enforcement activities.

Poynton: *Although Homeland Defense is, by definition, primarily focused on domestic activities for the prevention of, preparedness for, response to, and recovery from terrorism, major natural disasters, and other major emergencies, homeland defense begins far beyond U.S. borders. What initiatives did you undertake as Assistant Secretary to push the defense of the homeland as far out as possible?*

McHale: The truth is that I did nothing by myself. I was fortunate to work with an incredible team of professionals within DOD generally, and specifically within the Office of the Assistant Secretary of Defense for Homeland Defense and Americans' Security Affairs.

Homeland defense begins well beyond the borders of the U.S. and requires global connectivity. Working with DHS and other agencies, we were able to establish a system for intelligence collection, assessment, and dissemination that would provide early warning of emerging threats. The intent was to detect, identify, and defeat such threats as far away from the U.S. homeland as possible.

In addition to reorganizing and integrating intelligence assets, we established very close working relationships with partnering nations overseas. Our office had a particularly close relationship with the Israeli Defense Forces and specifically their Home Front Command. I routinely visited the Israelis during my time in office, observed their exercises, and noted their similarities to exercises then being conducted by NORTHCOM. In fact, we also arranged for Israeli, Mexican, and other representatives of foreign governments to observe, at an unclassified level, the ongoing exercises conducted by NORTHCOM. During the period of time I served as Assistant Secretary, the most serious threats to national security were often brought to our attention by partnering governments, allies, and friends overseas.

Poynton: *Eleven of the fifteen National Planning Scenarios provided by DHS involve a chemical, biological, radiological, nuclear, and explosive [CBRNE] attack. The Strategy for Homeland Defense and Civil Support, which you helped draft, states, "Terrorists and/or rogue states* ***will*** *[emphasis added] attempt multiple, simultaneous, mass-causality CBRNE attacks against the United States homeland." With recent events such as Syria's precarious stockpile of chemical weapons, do you still believe there is an inevitable likelihood of a weapon of mass destruction [WMD] attack on the homeland despite progress the United States has made over the past decade to detect, deter, and prevent such attacks?*

McHale: I believe it is a near certainty that such an attack will be attempted. The question is, over what timeframe? In the remaining decades of the 21st century, I find it difficult to believe that an adversary, either a nation state or a terrorist organization, will not attempt to employ WMD technology in an attack against the American people. The evolution of technology has now empowered terrorist organizations, and even individuals, with the destructive capacity that, in the past, could only be acquired by hostile nation states.

The 9/11 attack should serve as a case study in 21st-century asymmetric warfare. Despite having severely degraded the operational capability of Al-Qaida during the past decade, the type of attack launched on 9/11 is likely to remain a threat to the United States for many years to come. Indeed, Americans should not become complacent in the belief that the near defeat of Al-Qaida will eliminate the continuing threat of an asymmetric attack upon the United States employing highly destructive technology – most likely WMDs.

In my judgment, there has been a fundamental paradigm shift in the way warfare will be conducted in the future. Although the threat of a nation state adversary remains very real, I believe there is a much higher likelihood of asymmetric attacks, conducted against the American people here at home, for the purpose of degrading our political will and altering our national policies. In the case of Al-Qaida, our adversaries believed that American foreign policy could be changed by inflicting brutal acts of terrorism within U.S. borders. With the attack of 9/11 as an early precedent, hostile nation states and/or terrorist organizations – with increasing access to WMDs – are very likely to conduct asymmetric attacks against the U.S. homeland in the decades to come. We should not be frightened, but we must be prepared.

Poynton: *You co-founded the National Guard and Reserve Components Caucus, which advocates the interests of reservists and guardsmen worldwide. Several after-action reviews of the Hurricane Katrina response cited the integration between Title 10 [federally controlled] forces within the United States alongside the non-federalized Title 32 [State Active Duty National Guard] forces as an area that needed improvement. What has DOD done since then to ensure a more coordinated military response?*

McHale: Just a few days after Katrina made landfall in August 2005, I discussed with the secretary of defense my concerns regarding deficiencies in our nation's response. Although the military mission in response to Katrina was effective, I felt there were discrepancies in need of correction. Specifically, we recognized the

need for closer coordination between the Title 10 active duty members (NORTHCOM) and co-located Title 32 National Guard forces.

Since Katrina, there has been a lot of corrective action. We now have close coordination between the National Guard Bureau and NORTHCOM with regard to interoperability of communications equipment, unit training, and carefully coordinated DSCA deployment planning. It is extremely significant that Congress subsequently made the decision that the chief of the National Guard Bureau would become a 4-star officer – and more recently become a full voting member of the Joint Chiefs of Staff. And again by statute, Congress mandated that a deputy commander at NORTHCOM must be drawn from the Reserve component, specifically the National Guard. Today the deputy commander at NORTHCOM is a National Guard general officer, LTG Mike Dubie, the former Adjutant General of Vermont.

After Katrina, we also had full and thoughtful discussions with Secretary Rumsfeld on the use of dual status commanders – National Guard officers with concurrent authority over both Title 10 and Title 32 military forces. The secretary first authorized the so-called "dual status command" for the 2004 G-8 Summit at Sea Island, Georgia. BG Terry *Nesbitt*, a National Guard officer from Georgia was the first officer, at least in terms of modern authorities, placed in dual status command of all military forces that were deployed to enhance security at the G-8 Summit. The dual status commanders' training and certification that is now conducted ensures that National Guard officers – when placed in dual status – will be fully prepared for their duties.

Those kinds of institutional changes were put in place to ensure much closer coordination between the National Guard and Title 10 forces. The National Guard has done an extraordinary job over the past ten years in modernizing its forces. In terms of both doctrine and operational capacity, the National Guard has been at the forefront of military transformation in the realm of homeland defense and civil support – the CSTs [Civil Support Teams], the CERFPs [CBRNE enhanced response force packages], the Homeland Response Forces (HRFs), the improved coordination with NORTHCOM, and the EMAC [Emergency Management Assistance Compact] agreements between the governors – all ensure a more rapid and effective response in times of catastrophic disasters.

Poynton: *You just noted the transformational activities of the National Guard in this area. What is your level of confidence with regard to active component preparedness for disaster response?*

McHale: Although the National Guard has shown extraordinary vision in adapting to the new security environment of the 21st century, I am deeply concerned that federal capacity and planning are not where they need to be. Indeed, some changes made in recent years have actually diminished our ability to rapidly respond during and following a domestic disaster – for example, moving away from scenario-based planning (HSPD 8, Annex 1) to capability-based planning (PPD 8) was a mistake. Complex catastrophes require detailed plans and rigorous exercises. You cannot deploy thousands of personnel and tons of equipment on the fly – you had better have an executable base plan in place before the catastrophic event. Otherwise, your response will be too slow.

Unfortunately, the detailed operational plans needed to ensure a rapid, coordinated, and effective catastrophic

disaster response have yet to be written. Necessary planning should employ the full capacity of the federal government in close coordination with state and local capabilities, as well as the private sector. A system of capabilities-based planning simply offers an inventory of available assets, but assembling those assets to respond to a specific scenario – once it occurs – takes too much time to be effective. Delay costs lives. Additionally, the Department of the Army recently terminated its homeland defense and civil support planning cell, reassigning members of that cell to other units within the Department. That was an error.

There has also been a degradation of federal operational capacity. The 2010 QDR [Quadrennial Defense Review] terminated two-thirds of NORTHCOM's proposed operational capability. NORTHCOM was intended to have approximately 15,000 assigned forces to be used to assist DHS during and following any domestic disaster. However, the 2010 QDR cancelled two of NORTHCOM's proposed CBRNE consequence management response forces. There are also tentative plans to terminate the Marine Corps' CBIRF [Chemical Biological Incident Response Force] – a core NORTHCOM capability – no later than 2017. Hopefully, the Marine Corps will reconsider that decision.

As a result, the president currently has relatively few capabilities that are well trained and immediately available to NORTHCOM following a catastrophic event. By contrast, I believe the governors are well prepared and the National Guard has served the nation well in terms of developing innovative CBRNE response capabilities. Transformational changes within the National Guard ensure that governors have at their disposal substantial midrange CBRNE response capability. However, to work effectively with the National Guard, the men of women of NORTHCOM deserve better resourcing than they are now getting, including more assigned personnel, better training, and better equipment.

I believe the president is not well served by the current level of interagency planning and he does not have the capacity to rapidly and effectively respond to a domestic catastrophic event. Recent decisions have tended to diminish the commitment to and operational capacity for civil support missions. These choices – made in a constrained fiscal environment – have created unwarranted risk for the security of the American people. When taken in the aggregate, they significantly diminish our ability to execute homeland defense and civil support missions.

Poynton: *You once stated, "Hurricane Katrina was indeed, in my judgment, a catastrophic event; it was at the low end of catastrophic events in terms of tragic loss of life and destruction of property." Although the military response to the costliest hurricane in U.S. history was massive and impressive, the federal response in its entirety was largely viewed by the public as inadequate. If the response was in fact inadequate for this "low-end" catastrophic event, what would convince the American people to have confidence in an improved response to a more severe catastrophic event?*

McHale: We need to conduct very realistic national level exercises – with the full awareness of the American people and close congressional oversight. These exercises should demonstrate a capacity for effective disaster response. There also needs to be better planning oriented toward particular disaster scenarios and the necessary operational resources to confidently implement those plans – for example, a sufficient number of men and women with personal protective equipment, supported by well-drafted transportation and communications plans, able to achieve their assigned missions. With the necessary planning and resources in hand, the federal government needs to conduct routine national level exercises that will rigorously test both the operational plans and the adequacy of resources to ensure an effective response to a real world event.

If Americans observe such exercises being conducted on a routine basis, over time they will develop confidence in the U.S. capacity to effectively respond when a terrorist attack or a natural disaster actually occurs. At this point, however, I do not believe that existing plans are sufficient or that our operational capacity is adequate. In addition, current disaster exercises are insufficiently rigorous to realistically test preparedness levels. In each of these areas, although great progress has been made, there is room to significantly improve planning, strengthen operational resources, and conduct exercises that are more challenging, to gain the confidence of the American people and, when necessary, provide an effective response to future events.

Poynton: *You once recalled that, during your early days as a Marine, you gave your situation reports by radio transmission. In contrast, today's defense communications are sent electronically through a complex and vast cyber network. As a new critical infrastructure sector, such technologies increase efficiencies and create a number of other benefits, but also present vulnerabilities that are susceptible to terrorist attack. With a lack of comprehensive cyber security legislation – such as the recently defeated Cybersecurity Act of 2012 – how is DOD preparing for a potentially crippling cyber attack?*

McHale: I was deeply disappointed that Congress did not enact comprehensive cybersecurity legislation during the past session. As the end of the current Congress approaches, it looks very likely that the *Lieberman* Cybersecurity Bill and other cyber legislative initiatives will soon die, allowing very significant cyber vulnerabilities to remain unaddressed. I know this feeling of deep concern is shared by other members of the Aspen Homeland Security Group – a bipartisan group of foreign policy, homeland security, and counterterrorism experts under the leadership of my former House colleague Jane Harman and former secretary of DHS, Michael Chertoff. Members of the Aspen Group recently signed a letter to Congress expressing their concern that comprehensive cybersecurity legislation needs to be passed as quickly as possible. Unfortunately, that expression of concern appears to have had little effect.

I should note that DOD has shown considerable initiative in developing cyberdefense capabilities. Most prominently, the creation of the U.S. Cyber Command in 2009 has been the focal point of DOD's actions in his area. In my opinion, the cyber defense of the ".mil" domain is significantly stronger than parallel defensive capabilities within the ".com" world. Cyber Command draws upon many years of DOD experience in cyber communications and data transfer, as well as the experience of the National Security Agency. Although DOD seems to have taken appropriate steps to ensure the cybersecurity of the military domain, congressional authority will be required to effectively protect critical nodes of vulnerability within the civilian cyber infrastructure. To date, that kind of comprehensive approach to ensure the resilience of the civilian cyber infrastructure has not occurred. I hope the Congress returns to this issue with a renewed sense of urgency when the members of Congress resume their business in January.

Poynton: *It is a strategic assumption that transnational terrorists will attempt to gain surreptitious entry into the United States in order to launch an attack on the homeland. Despite thwarting some such attacks, there appears to be an increasing threat of domestic terrorism. A report last year by the U.S. Senate Committee on Homeland Security and Governmental Affairs called the Ft. Hood, Texas, shooting by U.S. Army Major Nidal Hasan "the worst terrorist attack on U.S. soil since September 11, 2001." Do you view this tragic shooting as an act of terrorism or an isolated criminal act? How has this event and other attempts of domestic terrorism affected DOD's strategy for homeland defense?*

McHale: An event like this is both an act of terror and a crime. The terms are not mutually exclusive, which is particularly clear in the case of Ft. Hood. The brutality of that attack should be seen as a terrorist attack and a violation of criminal law. That said, it would be a dangerous mistake to view such actions primarily from the standpoint of their criminal character.

Defending the American people here at home is, and should be, a duty primarily assigned to civilian law enforcement, but DOD is empowered by various statutes to provide support to civilian law enforcement agencies under very specific circumstances and the department must be prepared to do so when requested by those agencies and authorized by a relevant statute. It is only under extraordinary circumstances that military forces should be used on the ground to protect citizens on U.S. soil and, when that necessity arises, the military capacity employed should ordinarily be the National Guard. When such a crime occurs on U.S. soil, a prosecution should follow – but when justified by the facts, the isolated criminal event must be understood in the larger context of global terrorism. Domestic security cannot be achieved in the courtroom alone. It requires global vigilance.

Under almost all circumstances, however, the lead operational activity in providing security for the American people on the ground is properly entrusted to civilian law enforcement agencies.

Poynton: *Successfully protecting the homeland is contingent upon a strong partnership among industry, academia, and government. Based on your experience in both the government and the private sector, where do you see the greatest areas of collaboration among the three stakeholders in the years to come?*

McHale: I think that future collaboration will focus on critical infrastructure protection within the defense industrial base. DOD, which is heavily dependent on civilian infrastructure to effectively execute its priority missions, does not exist within a vacuum. Therefore, we likely will see a greater emphasis on critical nodes of vulnerability within the defense industrial base, ensuring that DOD will remain mission capable under any and all circumstances.

I also think there will be a close collaboration between DOD and DHS in terms of cyber security initiatives. DHS is the lead federal agency for the protection of the civilian cyber infrastructure; however, as noted earlier, DOD has considerable expertise in these areas. I am encouraged by the existing and evolving partnership between DOD and DHS, to make certain that whatever counsel DOD might provide to DHS is incorporated into an effective defense of civilian cyber infrastructure. DHS has the lead, but DOD can and should play an important supporting role.

Lastly, there likely will be closer coordination between DOD, industry, and academia with regard to the planning and execution of disaster response capabilities – especially following a catastrophic event. If there is a substantial terrorist attack against the U.S. homeland, or a severe natural disaster, an effective response will require close coordination among all levels of government and the private sector, with thoughtful analysis and planning assessments provided by academia. That kind of close integration of private and public sector capabilities to ensure an effective disaster response has not yet occurred. However, in the years ahead, there almost certainly will be a much closer level of cooperation to ensure that the capabilities found in each sector are coordinated and complementary. To be effective, each sector's capability should be fully incorporated into the planning process.

Paul McHale is the president of Civil Support International LLC, a consulting firm offering advisory services to government agencies and private contractors related to military sales, homeland defense, disaster preparedness, and crisis response. From 2003 to 2009, he served as Assistant Secretary of Defense for Homeland Defense, where he supervised all homeland defense activities for the U.S. Department of Defense (DoD). Prior to his appointment at DoD, he represented the 15th Congressional district of Pennsylvania in the U.S. House of Representatives from 1992 to 1998. Throughout that period, he was an active member of the House Armed Services Committee, which has oversight responsibility for all U.S. military operations and training. Additionally, he co-founded the National Guard and Reserve Components Caucus, served five terms in the Pennsylvania General Assembly, and is a retired colonel in the Marine Corps Reserve. He received his J.D. from Georgetown University Law Center and his B.A. with highest honors from Lehigh University.

Aaron Sean Poynton (pictured top left) is the Senior Government Market Specialist of Federal Programs at Thermo Fisher Scientific. Previously, he served as a director at Smiths Detection, a global technology company in the defense and homeland security markets. Prior to his civilian career, Aaron served in the U.S. Army as an enlisted special operations soldier and as an officer in the Chemical Corps. Dr. Poynton is a graduate of the Johns Hopkins University Army ROTC program and holds a bachelor's degree in economics from the University of Maryland UMBC, a master's degree from the George Washington University School of Business, and a doctorate in public administration from the University of Baltimore.

NANORAIDER™
Personal Spectroscopic Radiation Detector (SPRD-CZT)
for under than $10k

BECAUSE IT'S NOT JUST YOUR JOB, IT'S YOUR LIFE.™

The difference between life and death is in your hands. FLIR CBRNE threat detection products provide lab-caliber analysis where you need it most – in the field. When lives are at stake you need fast, accurate results you can trust.

FLIR®

www.FLIR.com/gs