



Mumbai

The Lessons Learned

The Mumbai Attacks - Lessons for the Western World

Joseph Trindal, Law Enforcement, Page 5

Mumbai: The Lessons Learned

What Not to Do -

Implications for the West

Neil C. Livingstone, Building Protection, Page 8

Emerging Infections And Their Impact on EMS

Raphael Barishansky, Public Health, Page 10

Changes and Clarifications - NIMS Upgrade Released

Stephen Grainer, Fire/HazMat, Page 13

The Field Testing Dilemma And LRN Chemical Laboratories

Richard France, Viewpoint, Page 17

Cold Calculations and The Search for Inner Warmth

Joseph Cahill, EMS, Page 19

How the NDMS Can Be Made More Effective

Michael Allswede, Public Health, Page 21

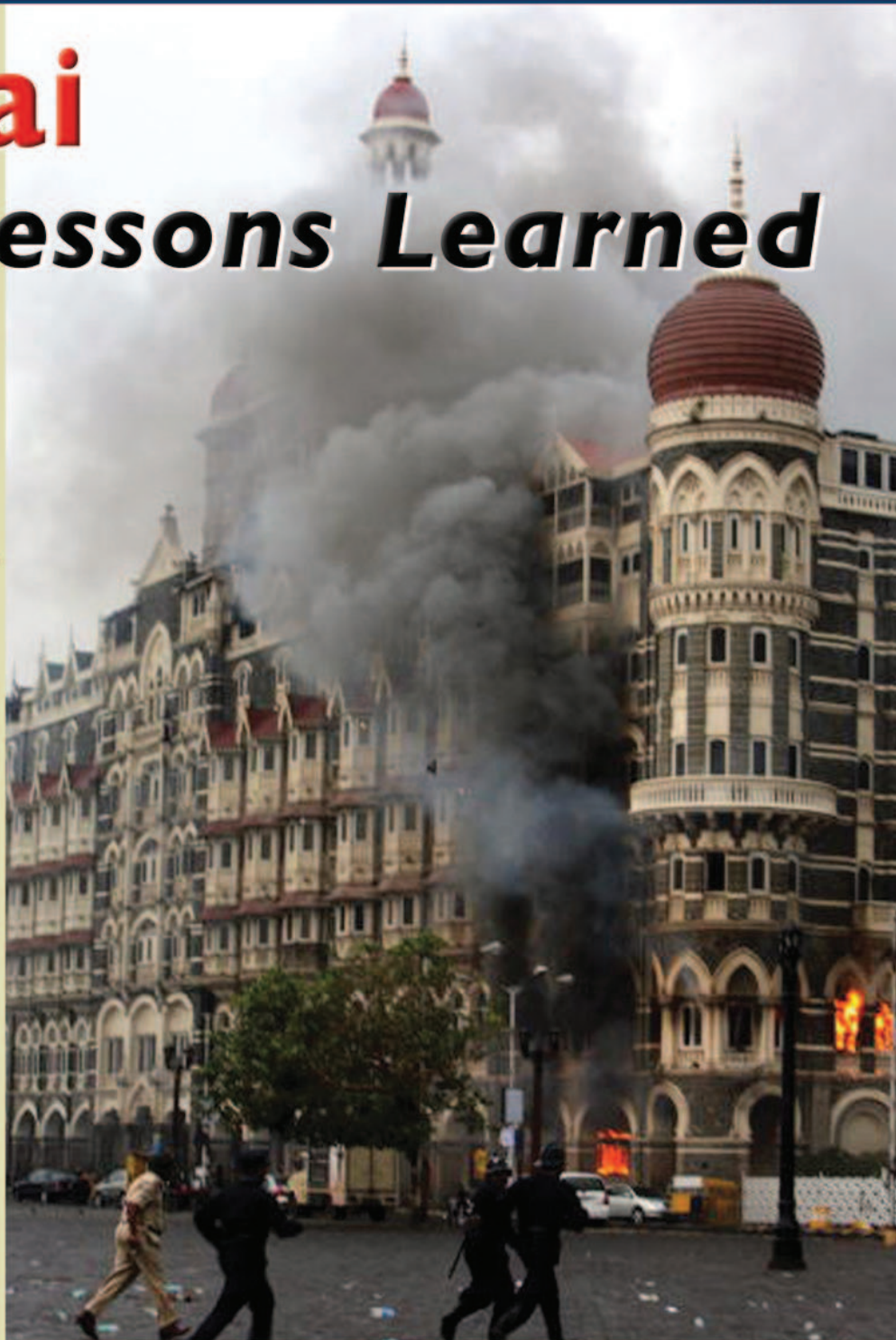
No Time to Cut Back on Safety - The Cost Is Too High

Warren K. Brown, Building Protection, Page 24

California, Ohio, Kansas, and Louisiana

Adam McLaughlin, State Homeland News
Page 25

For more details, visit:
DomesticPreparedness.com
Since 1998, Integrating Professional
Communities of Homeland Security



Subscription About to Expire?
Visit www.DomesticPreparedness.com
Enter Promo Code: RENEW
To extend your subscription

BIOLOGICAL AGENT IDENTIFICATION



A Perfect "10"

Test 10 Biothreat Agents Simultaneously

Now you can test for 10 deadly pathogens in less than 30 minutes. The 10™ Target Screen Kit comes with all of the items for sample gathering and testing for 10 of the most relevant pathogens related to bioterrorism.

Samples are analyzed on our Homeland Security-approved RAZOR® and RAZOR® EX instruments. This system identifies biological agents using DNA-based, field-proven PCR. Fast and easy to use, delivering reliable results every time.

The 10 Target Screen Kit is compatible with both the RAZOR EX and the original RAZOR system.

Anthrax
Tularemia
Brucella
Coxiella
E. coli O157
Botulism
Ricin
Salmonella
Smallpox
Plague



The RAZOR EX
with test pouch

The RAZOR EX Instrument comes with the following:

- + Bluetooth connection for PC data transfer, analysis, and archiving.
- + Large color screen and push button operation for use when wearing personal protective equipment (PPE).
- + Bar code reader for enhanced operability.

Visit us at www.idahotech.com
to learn more about our test kits
and to see our online video.

*Check Web site for additional tests.



**Idaho
Technology Inc.**

Innovative solutions for pathogen identification and DNA research

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

Business Office

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

Staff

Martin Masiuk
Publisher
mmasuk@domprep.com

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

John Morton
Strategic Advisor
jmorton@domprep.com

Dan Brethauer
Account Executive
dbrethauer@domprep.com

Susan Collins
Creative Director
scollins@domprep.com

Sharon Stovall
Editorial Director
sstovall@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

Advertisers in This Issue:

Disaster Response Recovery Expo
GovSec. U.S. Law & Ready Conference
ICx Technologies
Idaho Technology Inc.
IDGA Maritime Homeland Security Summit
MSA
PROENGINE Inc.

© Copyright 2009, by IMR Group, Inc.; reproduction of any part of this publication without express written permission is strictly prohibited.

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

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



Editor's Notes

By James D. Hessman, Editor in Chief



The principal focus of the Obama administration and the new Congress in the past two weeks, understandably, has been on spending – primarily to help jump-start the ailing U.S. economy by the infusion of hundreds of billions of dollars into the system over the next several months.

Inevitably, though, the attention of both the executive and legislative branches of government will reverse course and focus on ways to *reduce* spending, partly to offset the new “stimulus” increases, and partly because the funding priorities of the Obama administration differ considerably from those of the Bush administration – particularly, it seems likely, in the field of national defense. With the war in Iraq not yet completely over, but obviously winding down, at least *some* defense reductions are probably justified. But they should be very carefully calculated, prudently implemented, and administered in such a way that they do not cut into the core strengths of the nation’s armed services.

It should be clearly understood, moreover, that cutbacks in funding for the Department of Defense do not and should not be used as justification for similar cutbacks in the DHS (Department of Homeland Security) budget. Just the opposite, in fact. The two departments are partners in many ways, and in many of their activities. Their missions are complementary in some respects, but profoundly different in most ways.

Probably the most obvious difference is a geographic one. DOD focuses primarily on combat operations overseas. DHS’s sole focus is defending the U.S. homeland, and it carries out its mission primarily through *planning* and *preparedness*. Its goal is not to *win* battles per se, but to prevent them from starting. And in that context it seems obvious that it has probably been the most successful agency in government for more than seven years. A number of additional terrorist plots – some of them now public knowledge, but most of them classified – have been thwarted during that same time frame.

Which does not mean that the battle is over. Far from it. The United States still has a very long way to go before the American people can feel *reasonably* safe, and will probably never feel perfectly safe. For that reason alone, cutting DHS funding now, or at any time in the foreseeable future, would be equivalent to disarming the smoke detector because there has not been another fire since it was installed, or canceling a car-insurance policy because the driver has not had an accident recently.

The articles in this month’s printable issue of DPJ provide a microcosm of some of the important advances in preparedness recently accomplished – as well as a preview of some of the huge amount of difficult work that remains to be done: two articles, one by Joseph Trindal, the other by Neil Livingstone, on the Mumbai attacks and what not only India but the other nations of the Free World should learn from those attacks; timely articles by Joseph Cahill and Warren Brown on how cold weather and the lack of safety gear can hinder the effectiveness of the nation’s first responders; four short reports by Adam McLaughlin on recent homeland-security changes in California, Kansas, Louisiana, and Ohio; an article by Rick France on chemical-detection systems; and two policy analyses – by Stephen Grainer and Michael Allswede, respectively – on changes to the National Incident Management System and the National Disaster Medical System. Finally, Ray Barishansky provides a grim analysis of the escalating dangers posed by emerging infections.

About the Cover: Firefighters attend to a fire at the Taj Mahal Palace & Tower Hotel following the terrorist attacks in late November 2008 in Mumbai, India. Indian officials declared the siege over when the remaining militants were killed when commandos stormed the building. The “lessons learned” from the Mumbai attacks are discussed, from different perspectives, by Joseph Trindal and Neil Livingstone in this issue of DomPrep Journal. (Photo by India Today Group/Getty Images)

7th Annual

MARITIME HOMELAND SECURITY Summit

*Building Partnerships
for Maritime Security
and Enhanced
Domain Awareness*

April 27 – 30, 2009
Jacksonville, FL

DON'T MISS YOUR BEST OPPORTUNITY
OF THE YEAR TO:

- Hear the Coast Guard's current acquisition priorities and the impact on the maritime community
- Engage in the public-private joint effort to improve Maritime Domain Awareness
- Receive detailed updates and implementation strategies for critical capabilities

Get the Latest Update
on Coast Guard
Acquisition Priorities!

DomPrep Channel Masters

First Responders

Glen Rudner
Fire/HAZMAT

Stephen Grainer
Fire/HAZMAT

Joseph Cahill
EMS

Kay Goss
Emergency Management

Joseph Watson
Law Enforcement

Joseph Trindal
Law Enforcement

Rodrigo (Roddy) Moscoso
Law Enforcement

Medical Support

Jerry Mothershead
Hospital Administration

Michael Allswede
Public Health

Raphael Barishansky
Public Health

Updates

Adam McLaughlin
State Homeland News

Infrastructure

Neil Livingstone
ExecutiveAction

Funding & Regulations

Diana Hopkins
Standards

Borders & Ports

Joseph DiRenzo III
Coast Guard

Christopher Doane
Coast Guard

Military Support

Jonathan Dodson
National Guard

The Mumbai Attacks – Lessons for the Western World

By Joseph W. Trindal, Law Enforcement



The terrorist attacks two months ago in Mumbai provide a number of lessons for emergency-services agencies throughout the world. The attacks, which represented an ever-increasing level of sophistication and ingenuity of terrorist activity worldwide, started during the evening hours of 26 November 2008 when small teams of armed terrorists launched a well-coordinated series of assaults that challenged India's local and national emergency-services capabilities for four days.

The terrorist teams, which maintained radio communications with one another throughout the siege, moved swiftly and brazenly through the famous tourist city, initially firing on civilians and authorities alike before settling into hotels crowded with numerous Western tourists and business people. The last of the hostage/barricade situations was resolved on 30 November, leaving almost 200 fatalities and over 300 injured.

The terrorist tactics were relatively basic, but the overall operation was fairly sophisticated. In contrast, the response by local and national emergency-services agencies was much less coordinated. The terrorists used the now frequently experienced "multi-prong" approach by combining a number of IED (improvised explosive device) detonations in some areas with small-arms attacks in other areas. The separate teams used the small-arms fire to create a wider scope of carnage. The law-enforcement and military units responding

were frustrated in their heroic but somewhat ineffective efforts to locate and contain the terrorist commando teams.

The terrorist teams, using pre-programmed GPS devices, moved through Mumbai's maze of streets like experienced tour guides. There were only ten terrorists in all; divided into killing teams of two to four, they moved swiftly from one crowded target to another, using taxis and stolen vehicles, but sometimes on foot. At one point, a terrorist team commandeered a responding police vehicle, killing its occupants, including Maharashtra Police's Anti-Terrorism Squad chief, Hemant Karkare.

A Lack of Basic Intelligence

The Indian law-enforcement and military units responding lacked intelligence about the scope of the terror assault, the targets, and the weapons involved. Some responding units were simply disorganized; others were virtually paralyzed. One on-duty police commander (Senior Inspector Nagappa R. Mahale), however, swiftly set up roadblocks, a tactic that resulted in the interdiction of one of the terrorist commando teams.

That hasty roadblock, in fact – on Marine Drive on the way to Girgaum Chowpatty – captured the only terrorist to be taken alive. When one of the terrorists' stolen sedans turned onto Marine Drive en route to the next target, the driver realized that they were facing a police roadblock. During the attempt to turn around, a vicious firefight ensued between police and the terrorists. In an uncoordinated

albeit heroic effort to stop the terrorist team, officers assaulted the vehicle – however, as is customary in India, not all of the police officers were armed with firearms. But they fought with what they had. Sub-Inspector Tukaram Omble, despite being unarmed, clutched the barrel of an AK rifle held by terrorist Ajmal Amir Kasab; he absorbed six fatal shots, but other police officers clubbed Kasab into submission. Abu Ismail Khan, the other member of that terrorist team, was killed during the police counterattack.

Meanwhile, the other terrorist teams were continuing their attacks against key targets – the Taj Mahal Hotel, the Oberoi Hotel (formerly known as the Trident), and the Nariman House (also known as the Chabad House Jewish Center). All of the terrorist teams seemed to have a very good understanding of the layouts of all of their targets. During the course of the various assaults, the terrorist teams gathered hostages and even established command posts in hotel rooms. The local and state law-enforcement and military units responding eventually contained all of the terrorist refuges, and the battle became a fixed-barricade hostage situation.

Eyewitness accounts and the evidence collected to date indicate that the terrorist teams were in communications with one another as well as with command oversight elements beyond India's borders. In addition, it seems evident that some of the terrorist team leaders possessed the hand-held devices needed to gather real-time intelligence through internet-based news media reports. Conversely, most if not all of the local and national police and military units responding seemed to lack even basic communications interoperability. There also was an almost total lack

of command and control between and among the responding units.

Moreover, unlike the terrorist teams, the police and military commanders had little or no real-time understanding of a common operating picture during much of this deadly and rapidly moving event. Eventually, though, after the terrorist teams had settled into known locations, the Indian containment and interdiction actions became reasonably well organized – and thus more cohesive and effective. Ultimately, the terrorist

800 police, Indian National Security Guards, and military personnel worked together to isolate, contain, and resolve the attacks of 10 terrorists

commando teams were neutralized through coordinated military and police small-unit operations. At the end of the four-day siege there were more than 800 police, Indian National Security Guards (NSGs), and military personnel working together in Mumbai to isolate, contain, and resolve the attacks of 10 terrorists, who had split up into four coordinated killer teams.

The Mumbai Medical System: Overworked & Underprepared

The Mumbai emergency medical system was not prepared for an event in which many of the casualties were self-evacuating to area hospitals – and in which hospitals were also on the terrorist target list. Cama Hospital, for

example, was in the midst of receiving injured patients when the terrorist team led by Abu Ismail Khan opened fire at the hospital.

It turned out that this attack was little more than a drive-by shooting; nonetheless, it heightened an already chaotic situation. Many of the on-scene victims were assisted by other citizens; a number of them were transported from the immediate danger areas on luggage carts or dollies, or were even carried by other citizens who were on the scene but had not been injured. Because there were not enough ambulances available, transportation for some victims was provided by private motorcars.

In addition, there was little if any on-scene triage carried out, and no hospital “distribution plan” had been set up. As a result, patients lined the corridors and hallways as three area hospitals tried feverishly to manage a major spike in critical-care demand – in a medical-care system that is routinely stretched to the limit. Some victims died in transit; others died while awaiting care.

Lethal Carnage And Deadly Lessons

Despite the widespread carnage and the lives lost, there were some valuable lessons learned as well – including the following:

1. Coordinated multi-prong attack methodologies should be expected and studied by all emergency-services agencies and jurisdictions. Mumbai is not the first multi-target attack of its type and certainly will not be the last. Terrorist planners recognize the effectiveness of these types of attacks in straining the emergency-services systems of their chosen targets.

2. Attack planning and preparations should involve all emergency-services agencies as well as potential private-sector targets. The Mumbai attack operationally targeted hotels (the Oberoi and the Taj Mahal), public transportation services (taxis & rail), hospitals, and dining and entertainment venues (the Metro Cinema & Café Leopold) as well as a religious-oriented community center (Nariman House). In addition, the terrorist commandos were mentally and operationally prepared for dramatic encounters with the law-enforcement and military personnel who responded. The latter point was underscored by Kasab and Khan's hasty ambush of a responding police vehicle; the ambush resulted in the death of Maharashtra Anti-Terrorism Chief Hemant Karhare and two other police officers. Rather than remaining hidden and let the police vehicle pass by safely, running its lights and siren furiously, the terrorists chose the brazen tactic of assaulting the police directly.

3. Communications interoperability should be expanded, tested, and significantly improved. Communication challenges have been identified in the United States, and in other Western countries, as a consistent emergency-services coordination soft spot. India's police and military communications interoperability is almost non-existent. Nonetheless, facing a rapidly evolving coordinated assault similar to the Mumbai attack, even most U.S. agencies would be challenged to implement communications interoperability plans with mutual-aid partners rapidly enough to effectively blunt a similar attack.

4. Closely associated with the need for improved communications is

a parallel need to rapidly develop accurate, real-time situational awareness and provide a common operating picture between responding emergency services disciplines and jurisdictions. In Mumbai, the terrorist teams worked effectively to maintain an accurate situational awareness of most local and area law-enforcement and military-response operations. When their efforts were effective, they were able to stay ahead of the public service interdiction efforts. A case in point was that the terrorists obviously had a better understanding of the Taj Mahal Hotel's floor plan than the responding police and military units did. Witnesses described several instances in which the terrorists would "disappear" only to re-appear in areas that had already been swept by police and military units. This cat-and-mouse challenge generated additional confusion for the police and military officials, many of whom believed the number of terrorists in the Taj Mahal Hotel was much greater than it actually was.

5. Private-sector businesses must be encouraged to participate in emergency-preparedness activities. There was no coordinated plan linking local police and anti-terrorism units with the private-sector targets of the Mumbai terrorist teams. The attacks were initiated after business hours, and under the cover of darkness. Private-sector business preparedness should include those personnel assigned on *all* shifts. Most businesses are unprepared for an armed assault, and many are reluctant to take time out of their daily business operations to plan and prepare for such assaults. However, a higher-level objective of the Mumbai attack was to target the tourist

industry in Mumbai, and India as a whole. At the strategic level, this intensity of pressure, because of the importance of tourism to the Indian economy, was probably designed to escalate tensions between India and Pakistan. Private-sector infrastructure assets have historically been attractive targets for terrorist groups in achieving broader strategic objectives. From a profitability point of view, the lack of preparedness to safeguard customers makes poor business sense in the 21st century. The Mumbai attacks – in which private businesses were once again a soft terrorist target – should be another warning to public officials and business leaders alike.

In short, the complexity and deadly nature of the Mumbai attacks raises the bar of terrorist operational capabilities worldwide. Seen in that context, the terrorist assault on Mumbai ranks on the same plane as the Moscow Theater siege, the attacks on London's underground subway system, and the 11 September 2001 terrorist attacks on the Pentagon and the World Trade Center towers. All were watershed events in the global evolution of terrorist campaigns against the democratic societies of the Western world. Emergency-services planners and public officials should closely study the Mumbai attacks, therefore, with an objective of elevating their emergency preparedness and response posture to a new level that embraces the private sector as well as the entire spectrum of emergency-services disciplines.

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

Mumbai: The Lessons Learned

What Not to Do – Implications for the West

By Neil C. Livingstone, Viewpoint



Less than two months ago – in late November 2008 – terrorists carried out a series of coordinated attacks across Mumbai,

India, that resulted in 173 killed (the exact number is still disputed) and another 308 injured. At least six Americans were among the dead. The incident, which lasted for 62 hours and stretched over four days, brought India's largest city, and financial center, to a virtual standstill.

Initially, because of the scale of the attacks and the mayhem that ensued, it was believed that there were 15 to 25 terrorists actively participating in the attacks – but later intelligence suggested that the number was closer to ten. In the aftermath of the bloody incident, Indian officials blamed Pakistan, its traditional rival – and, like India, the possessor of nuclear weapons. India and Pakistan have fought three wars since the independence of the two nations. Only one terrorist is known to have survived the operation, a Pakistani named Ajmal Qasab, who indicated during his interrogation that he was a member of a group called Lashkar-e-Taiba and had been trained at a camp in Pakistan.

Pakistan clearly bears at least part of the blame, because all nations are prohibited under international law from allowing their territory to be used by armed militants to carry out attacks on other countries. Nevertheless, India also must share some responsibility for the attacks, primarily because its response to the crisis was nothing short of disastrous.

Mistakes, Malfunctions, And Misunderstandings

Not only was India wholly unprepared for the terrorist assault, despite growing domestic violence in recent years, but its performance once the attacks were underway is reminiscent of other botched attempts, by other governments, to address previous hostage crises – most notably, perhaps, the debacle at the 1972 Munich Olympics

Some Indian police officers demonstrated commendable bravery, but many of their actions were uncoordinated and, in some situations, counterproductive

in what was then West Germany. During the Summer Olympics in Munich, a group of Black September (Palestinian) terrorists infiltrated the Olympic village and took hostage a number of Israeli athletes and coaches. West Germany responded by attempting to rescue the hostages – after first luring the terrorists, and their captives, to a nearby airfield and promising them a safe exit. The West German government had refused to permit well-trained Israeli commandos from launching a rescue operation and instead had relied on poorly trained and equipped police to carry out the mission. Because of Germany's Nazi past, the better-prepared West German military was banned under the constitution from operating inside the country.

The West German police had no actual “plan” as such for rescuing the hostages, but simply deployed five snipers to take out the terrorists. There were fewer snipers than there were terrorists, though, and none of the snipers was a trained sharpshooter. Moreover, their weapons were substandard, especially in low-light situations, and they lacked not only body armor and helmets but also the radios they needed to keep them abreast of developments in what was an extremely tense and very fluid situation. In addition, the helicopters carrying the terrorists and their hostages to the airport landed in the wrong place, blocking clear shots by the snipers and giving the terrorists some obviously unintended cover.

The snipers opened fire but initially killed only two of the terrorists. The remaining terrorists then returned fire – while also proceeding to systematically murder nine Israeli hostages, who were bound and helpless in the helicopters, with gunfire and grenades. Two other Israelis had been killed during the takeover of the Israeli compound. When the incident was finally over, five terrorists were dead and three others were in custody. A German police officer also had been killed.

Reeling from international criticism of its handling of the crisis, the West German government undertook a number of reforms – including the creation of the elite anti-terrorist GSG-9 commando unit – to ensure that it would never again be caught unprepared by terrorists.

Mumbai Parallels – Compounded

India's response to the 26 November 2008 terrorist attacks was eerily

reminiscent of the botched West German response 36 years earlier. Although Indian intelligence had warned management of the two principal targets – the Trident Oberoi and Taj Mahal Palace & Tower hotels – of a possible terrorist attack, both hotels had beefed up security only temporarily, but returned to business as usual when nothing happened. The Indian government failed, moreover, to take any steps to increase security at Mumbai's seaport facilities. The attackers, it turned out, reached Mumbai via speed boats that had been launched from trawlers. Mumbai is believed to have 15 patrol boats in its waterfront inventory, but none of them, according to reports, were used for patrolling.

It is now believed there were only ten attackers, a relatively small number considering the widespread havoc they caused, but they not only were well-armed – with explosives and small arms – but also were equipped with GPS systems, body armor, and cell phones. Prior to the attacks, moreover, confederates of the terrorists apparently had carried out an extensive recon of all of the projected targets and the attackers had studied the recon information both on-line and using Google Earth.

The terrorists hit ten targets in all, but the two hotels clearly were their principal objectives. Hostages were taken at both hotels, and at a Jewish center known as the Nariman House. The Indian government responded tentatively and without effective coordination between the Mumbai police and government security forces. The coordination problems apparently were complicated, at least in part, by the fact that Mumbai lost three top anti-terrorism officials early in the crisis when their van was ambushed by the terrorists.

The city of Mumbai has no rapid-response anti-terrorism or SWAT

(Special Weapons and Tactics) unit, so – after much hand-wringing and bureaucratic bickering – a federal unit, the Marine Commando Force (MCF), was activated. But the MCF is based in India's capital, New Delhi, which is three hours away from Mumbai by air, and some reports suggest that the Indian Navy wanted a written request from the government before it would release the commandos for the operation.

A further complication was that the MCF has no dedicated aviation resources of its own, or even the authority to requisition a commercial aircraft, and was forced to wait for a military transport to be dispatched from another location. Moreover, once the MCF reached Mumbai, the local transport it was provided was in the form of buses rather than helicopters. The bottom line is that it took nine hours for the government commandos to reach the scene, and it is not unfair to suggest that each hour's delay clearly resulted in more casualties.

The local police who initially responded to the attacks – and for hours were the only security forces on the scene – were hampered by inadequate communications. In addition, they possessed only limited body armor (which was improperly strapped on), substandard weapons, few if any scopes for their rifles, and no night-vision equipment. It goes without saying that they also lacked flash-bang grenades, pin-hole cameras, robots that could be used to search for and detonate explosives, and equipment that reads the heat-signatures of bodies; all of these and other high-tech equipment items are now standard issue for Western SWAT and elite anti-terrorism units.

The local police also were not trained in room-clearing operations and/or hostage negotiations. Some individual Indian police officers

demonstrated commendable bravery, but many of their actions were uncoordinated and even, in some situations, counterproductive. In several locations, the Mumbai police even failed to set up adequate perimeters around the attack sites.

In the weeks following the attacks, the Indian government has been under fire, both at home and abroad, for its slow and incompetent response. Home Minister Shivraj Patil and India's national security advisor both resigned in the wake of the Mumbai debacle. Today, India appears to be raising tensions with Pakistan as a way of deflecting attention from its own poor performance, both before and after the attacks. There have been a number of calls for ratcheting up India's counter-terrorism capabilities, but many observers despair, saying that bureaucratic inertia and corruption would likely hamstring any substantial reform.

Western intelligence and counterterrorism services are already incorporating the "lessons learned" from Mumbai into their own training curricula and op orders. If there are any lessons for India itself from the Mumbai crisis it is that the Indian government must be much better prepared to cope with future attacks, that it must create and adequately fund its own dedicated counter-terrorist resources – as well as a clear command and control system to manage such incidents – and that it must provide significantly more financial and other assistance to local counter-terrorist forces. Only in this way will India be able to respond immediately and effectively to future terrorist attacks.

Dr. Neil C. Livingstone, chairman and CEO of Executive Action LLC and an internationally respected expert in terrorism and counterterrorism, homeland defense, foreign policy, and national security, has written nine books and more than 200 articles in those fields.

Emerging Infections and Their Impact on EMS

By Raphael Barishansky, Public Health



Small pox; Tuberculosis; Polio – All were once classified as “emerging infections” and under that name ravaged populations in the United States and many other countries. The development of vaccines and treatment modalities worked to erase them from Western health concerns – but lack of health care in Third World countries, lax security at bio-stock facilities in the former Soviet Union, and the appearance of new drug-resistant strains of infections are breathing new life into these and other “old” threats.

Monkeypox; Ebola Virus; SARS – As global travel and the expansion of commerce continue to make the world an ever closer community, these previously isolated illnesses find themselves carried across oceans and continents, often without warning, within days of their initial outbreak. Which brings up an immensely important question: What are the responsibilities of emergency medical services (EMS) organizations and agencies in the field of emerging infections?

To answer that question one might start with the generic definition of *Emerging Infection* offered by the National Association of Emergency Medical Technicians in a 2005 position paper that described it as “a new, reemerging, or drug-resistant infection whose incidence in humans has increased within the past two decades or threatens to increase in the near future.” That definition not only encompasses the diseases mentioned above but also brings to mind certain other well-known infections such as Multi-Drug-Resistant Tuberculosis (MDR-TB) and HIV/AIDS.

Another recent definition/classification, this one from Columbia University, refers to three circumstances that indicate the presence of an emerging infection – namely, that it is either: (1) a new previously unknown infectious agent or disease; or (2) a previously described infectious agent in a new geographic location, as a new syndrome, in a new type of host, or with an increased drug-resistant pattern or other new genetic characteristic; or (3) a new or previously described infectious agent used as a bioweapon.

Their Own Worst Enemy

According to statistics compiled and maintained by the federal Centers for Disease Control and Prevention (CDC), Western healthcare is not only an essential part of the solution in the battle against emerging diseases but also, unfortunately, often a key part of the problem as well. The failure to follow well established personal and patient protective protocols as simple as the washing of one’s hands and the wearing of respiratory personal protective equipment (PPE) has led to a significant increase in healthcare-associated infections in the United States itself, where approximately 1.8 million hospitalized patients are infected annually, and 88,000 die as a result.

Five principal pathogens are associated with about half of all of the reported infections. The 2003 Sudden Acute Respiratory Syndrome (SARS) epidemic, which caused numerous deaths in Taiwan and Canada, demonstrated how just one emerging pathogen could have a profound impact by serving as a healthcare-associated infection. The healthcare-associated transmission

of SARS was considered to be the primary accelerator of the disease in both of the countries named.

The SARS experience represents the confluence of emerging-infections issues and patient-safety issues. The continued awareness of and search for healthcare-associated infections is therefore a key factor both in preventing the emergence of infectious diseases and in improving patient safety.

A Focus On Syndromic Surveillance

As has been suggested by the World Health Organization, an emerging infection will probably not be immediately recognized as such. This is one of the principal reasons why EMS systems must endeavor to participate in public-health and emergency-management monitoring activities. “Syndromic surveillance” – a recent and rapidly developing procedure defined by the CDC as “using health-related data that precede diagnosis and signal a sufficient probability of a case or an outbreak to warrant further public health response” – is proving to be a key tool in this effort. As used in the EMS field, syndromic surveillance involves the live analysis of data – e.g., 911 calls and dispatch data – to identify patterns and trends *as they emerge*, rather than waiting days or even weeks for conventional detection methods, such as the one-by-one review of patient charts, to provide actionable evidence. The variables or triggers for a natural epidemic and/or an artificially induced disease threat would include any cluster of pre-determined key symptoms such as breathing difficulties, abdominal pain, or fever accompanied by a rash.



AirSentinel®
CONTINUOUS BIOLOGICAL
AIR MONITORING



StarWatch SMS™
SECURITY MANAGEMENT
SYSTEM



Fido®
HANDHELD EXPLOSIVES
DETECTION



stanchionSPEC™
STATIONARY RADIATION
IDENTIFICATION SYSTEM



ADVANCED CAPABILITIES FOR CRITICAL ASSET PROTECTION

ICx Technologies is a leader in the development and integration of advanced detection technologies for all the CBRNE segments. Our sensors are compact, portable and simple to use. These network ready CBRNE detection instruments are ultra sensitive, accurate and have low false alarm rates. Our ruggedized products deliver the situational awareness and actionable intelligence necessary for facility and checkpoint monitoring such as at the Statue of Liberty and Ellis Island in New York.

Early detection allows appropriate action to be taken more quickly, not only saving lives but also protecting the healthcare infrastructure. Unlike the conventional syndromic surveillance data sources used in public health monitoring – or similar reports developed from private physician visits and/or the “patterning” of pharmaceutical purchases – EMS dispatch data is not only exceptionally time-sensitive but also systematically links gathered information with medical symptoms and provides an accurate geographic “distribution map” of disease incidents.

A growing number of cities across the United States have already started to use syndromic-surveillance technology and/or procedures to develop early-warning notifications on various clusters of patients suffering from specific illnesses or injuries, and this practice has thus far performed above expectations. The possibility of developing a nationwide syndromic-surveillance network within the foreseeable future is therefore no longer a concept but an achievable goal.

Protection for EMS Providers a High Priority

Individual EMS providers can actually do something personally about emerging infections. Following the suspicion of the SARS outbreak, governmental authorities overseas immediately instituted certain policies, including the use of full PPE gear for each EMS provider, as well as specific training – in infection-control techniques, for example – and frequent updates on the general situation to protect EMS personnel. The importance of developing and emphasizing personal awareness and preparedness cannot be overstated, and encompasses

everything from paying attention to the public-health updates provided around EMS stations and/or medical-control facilities to knowing where PPE masks and other gear are stored in an EMS unit to considering the principal complaints and symptoms of patients not only individually but also collectively.

The continued awareness of and search for healthcare-associated infections is a key factor both in preventing the emergence of infectious diseases and in improving patient safety

Here it should be noted that an important but frequently overlooked aspect of an EMS provider’s assessment is the reconciling of pertinent signs and symptoms with the individual patient’s recent travel history (which countries, and when, has the patient visited?) as well as other anecdotal evidence – contact with certain animals, for example – that might indicate the presence of an infectious disease.

Another common-sense test would be to ascertain if there is an unusual increase in the number of patients with common complaints, especially when those patients represent different groups (male vs. female, for example, or old vs. young). The EMS provider should make it a habit to speak to the nurses and doctors at local emergency departments and ask them if they have been seeing the

same clustering of symptoms.

The list of protection requirements for EMS must also, of course, include paying strict attention to the basic rules of medical hygiene, including but not limited to the following:

- The use of appropriate PPE – this means gloves, gowns, and a mask with eye protection (and preferably a face shield); after use these items must be treated as medical waste and disposed of properly;
- A requirement that EMS providers ensure that appropriate PPE is provided for patients; if there are concerns about a possible airborne contagion, the patients must wear either non-rebreather masks or surgical masks; contact with skin lesions can be minimized by wrapping the body part with loose gauze, or the entire patient with a clean sheet;
- An insistence that EMS providers thoroughly clean all of the vehicles used after every call – “thoroughly” includes the use of suitable disinfectants, and “vehicles” refers to all non-disposable equipment that was used as well as the surfaces of the vehicle itself;
- Finally, a similar insistence that EMS providers wash their hands after *every* patient contact. (The use of alcohol-based disinfectants is acceptable for the short term, but as soon as possible the EMS provider must wash his or her hands thoroughly with soap and tepid water, remembering to clean under the nails.)

To briefly summarize: Previously unseen and/or metamorphosed infections are making themselves known all of the time. Just over four years ago – on 18 February

2005, specifically – two separate and apparently unrelated disease outbreaks were reported in the *New York Times*. One involved more than 400 people near Amsterdam who had tested positive for TB following contact with an infected supermarket cashier. More frightening was the fact that an additional 21,000 people were reported to have possibly come in contact with the 400 already identified. The other case focused on an outbreak of rare pneumonic plague in the Congo that killed over 60 people and had possibly infected hundreds more. Several thousand workers self-evacuated the area without follow-up with medical authorities, fleeing “into the forests,” the *Times* reported, “to escape the highly contagious disease.”

EMS systems, and the providers who operate in them, cannot afford to live in the proverbial vacuum. What the new emergence of so many infectious diseases means for EMS agencies, their staffs, administrators, and medical directors is that there is a much increased need for real-time information about emerging infections; that need translates into: (a) consistent communications with relevant health-care authorities; (b) the constant updating of policies and procedures to reflect realities such as those described above; and (c) a requirement that EMS providers themselves stay constantly vigilant in developing and following up on their own assessments and not be lulled into thinking that “it’s *only* the flu.”

Raphael M. Barishansky, MPH, is currently the Program Chief for Public Health Emergency Preparedness for the Prince George’s County (Md.) Department of Health. Prior to establishing himself in this position, he served as Executive Director of the Hudson Valley Regional EMS (Emergency Medical Services) Council, based in Newburgh, N.Y.

Changes and Clarifications – NIMS Upgrade Released

By Stephen Grainer, Fire/HazMat



On 18 December 2008, long-awaited revisions to the National Incident Management System (NIMS) – officially described as an “upgrade” by the former acting director of the NIMS Integration Center, Albert Fluman – were published by the Department of Homeland Security (DHS) and are now being implemented.

The effort to improve the original template for the NIMS actually began early in 2006. A stakeholder working group that included more than 100 of the most actively involved and experienced representatives of various federal agencies – as well as state and local governments, tribal nations, the U.S. military, and various non-government organizations (NGOs) – worked together in a series of meetings designed to carry out one basic task: dissect, evaluate, and reassemble the NIMS in such a way that it would: (a) be more understandable; (b) be more applicable across a broad spectrum of incidents and events; and (c) provide a stronger degree of cohesion among the many stakeholders.

The net outcome, participants said, is a document that more clearly captures the intent as well as the mechanisms for implementing a true National Incident Management System. What follows is a capsule summary of the more significant changes and upgrades included in the December 2008 revision of the NIMS.

Reorientation, Realignment, & Restructuring

The initial NIMS document consisted of six primary components: *Command & Management; Preparedness; Resource Management; Communications and Information Management; Supporting Technologies; and On-Going Management and Maintenance*. Although these major components remain an integral part of the basic NIMS concept, a careful and lengthy analysis of their relationships with one another led to the determination that a reorientation was necessary to more effectively align each and all of them with the original NIMS policy guidelines.

This was done by first restructuring the organizational framework of the system – the document – to more accurately reflect the working and conceptual relationships between and among the six primary components named above. The *Command and Management* component was the first and predominant element of the initial NIMS, but the general feeling of the stakeholder representatives was that Command and Management – particularly as manifested in the Incident Command System (ICS) – was primarily an *outcome* of thorough and effective *Preparedness*. Preparedness itself, of course, includes training, exercises, and planning – all of which are necessary to develop and maintain proficiency in command and management skills.

The next step was formally recognizing that Command and Management cannot be effectively executed without



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

Co-located with the MRC, OFRD, ESAR-VHP and NDMS Training Event, the **2009 Disaster Response & Recovery Exposition** is the perfect opportunity for public health and emergency preparedness practitioners and policy makers to discover the latest equipment, technologies and services available.

- Communications Equipment
- Computer Software/Hardware
- Decontamination Shelters & Equipment
- Emergency Lighting
- Health Care Systems
- Information Technology
- Hazmat Response Equipment
- Medical Supplies and Equipment
- Pharmaceuticals
- Public Health & Safety
- Public Works
- Rescue Equipment
- Safety Equipment
- Shelters
- Social Services
- Vehicles
- And More!

For more information or to become an exhibitor, contact:

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

+ Disaster
Response and Recovery EXPO

Co-located with the MRC, OFRD, ESAR-VHP and NDMS Training Event

REGISTER TO ATTEND TODAY! VISIT WWW.DRREXPO.COM

APRIL 5-7, 2009 • HILTON ANATOLE, DALLAS, TEXAS

resources – and, therefore, effective *Resource Management*. Resource Management, however, is not simply a matter of possessing sufficient resources and assigning them in a command context. It also encompasses, among other things: establishing performance standards and qualifications; inventorying prior to need; maintaining the resources available in an operational (ready) condition; and having a systematic means to acquire, deploy, track, and eventually demobilize those resources.

After further deliberation the stakeholder participants also determined that Command and Management are reliant on effective *Communications and Information Management*. In order to be successful in Command and Management, obviously, an Incident Commander (IC) must be fully aware of the situation, able to manage the information flowing to and from the command element, and to communicate both concisely and effectively.

After several months of intense analysis and discussion, the working group recommended that the NIMS concept itself be re-formatted to focus primarily on Preparedness, Communications and Information Management, and Resource Management – which would be followed on the conceptual priority list by Command and Management and, finally, On-Going Management and Maintenance. The revised NIMS document consists of those elements, in that order, and therefore more accurately reflects the “life-cycle” or systematic process underpinning the National Incident Management System.

Here it should be noted that the *Supporting Technology* component of the original NIMS is not included

in the order of “chapters” in the revised NIMS. During the analysis it was debated how Supporting Technology could best be used in executing the NIMS principles and concepts. It was agreed that, although technology is a valuable component of all aspects of the NIMS document, the most valuable application of Supporting Technology was, is, and should be in the overall *Maintenance and*

Management encompasses, among other things, establishing performance standards and qualifications and having a systematic means to acquire, deploy, track, and eventually demobilize those resources

Management of NIMS. For that reason, Supporting Technology was incorporated as a primary mechanism for ensuring On-Going Management and Maintenance. Thus, all of the primary NIMS components were realigned to more accurately reflect the structure and concepts of the process that NIMS is intended to provide as the basis for improved interoperability and compatibility among all response organizations.

Greater Depth And Additional Clarifications

Another important revision was the development of added “depth” for each of the components

listed above. In the Preparedness component, for example, greater discussion is directed to the relationship between NIMS and the National Response Framework (NRF). (Note: the efforts to revise and upgrade the NIMS document were conducted concurrently with similar efforts to revise and improve the National Response Plan (NRP). Those efforts resulted in a parallel reconfiguration of the NRP and the evolution of the National Response Framework.) The Preparedness component also includes suggested actions that can be taken by preparedness organizations to more effectively apply the NIMS concepts and principles.

Perhaps one of the most important aspects of the improvements in the revised NIMS is a discussion of the roles and activities of elected and appointed officials. The numerous ways in which these officials are involved in the implementation of NIMS also are included in the Preparedness component, and are a valuable addition to the original NIMS policy statement. Here it is worth pointing out that, although it may have been assumed in the original development of NIMS that elected and appointed officials would recognize and understand their important roles, the absence of any guidelines or delineation of those roles led to considerable confusion. It is expected that the additional information now provided will alleviate much of the previous uncertainty.

The revised NIMS document also includes an expanded section focused on the relationship between NIMS and other preparedness efforts – including, for example, identifying and describing how NIMS is integrated with other Homeland Security Presidential Directives such as HSPD-7,

“Critical Infrastructure Identification Prioritization and Protection.” The NIMS relationship with HSPD-8, “National Preparedness,” also is clarified by identifying the direct relationship between national preparedness and the preparedness component of the revised NIMS policy statement. And, although the National Response Plan was referenced in the initial NIMS draft, the revised document more clearly establishes the closer NIMS relationship with the new National Response Framework.

An important technical clarification was made in the Command and Management component that has led to additional refinements (currently under way). Within the ICS element of Command and Management a new function was identified. That function was initially referred to as “Intelligence and Information.” As those already familiar with NIMS may recall, it was reasoned that in many potential scenarios the collection, analysis, and dissemination of intelligence (or “information”) related to the cause and effect of a particular situation or incident might be a critical element in effectively managing that incident. However, the use of the term “information” created confusion among less-experienced ICS practitioners. The greatest confusion was about which “information” was being referenced – i.e., information such as “public information,” or information that is important to

incident commanders but – for security reasons, primarily – should not be divulged to the general public.

To avoid future misunderstandings of this type, the terminology was changed. The function of “Intelligence and Information” in the ICS became “Intelligence and Investigations.” This change in nomenclature has helped to more clearly distinguish between “Public Information” and “Incident Information” or “Intelligence.” Because of the technical distinctions involved, this change also led the reviewers to recommend that a separate working group be established to develop guidance and protocols for the newly coined Intelligence and Investigations function. That working group has recently released its first public draft of the guidance for review.

Perhaps one of the most useful modifications to the revised NIMS is the greatly expanded incorporation of diagrams and graphics to support the text. The initial NIMS can accurately be characterized as “dry” reading. In addition to the use of “jump boxes” to highlight key points, numerous diagrams in the new document provide readers with a visual description of the points presented. Throughout the revised document, the user gets the feeling that NIMS is not merely a “concept paper” but is, rather, a document that the user can readily reference.

Finally, and largely as a result of the

input provided by the stakeholder representatives, the revisions incorporated in the new document reflect an effort to truly simplify the core components of NIMS. Rather than detailing intricacies of the components within each “chapter,” those details were transferred to a greatly expanded set of appendices to the core document. For the user who needs only a fundamental appreciation of NIMS, the “devil in the details” is re-located to an appropriate appendix. However, references for additional details are included in the core text to enable those who need, or seek, more information to easily locate those details.

In summary, the revised NIMS reflects a wealth of important information that more clearly defines the doctrine, scope, intent, and mechanisms of a truly useful National Incident Management System. Most users will find the content, format, and design to be an appreciable improvement over the original NIMS document.

To review the entire text of the NIMS revisions, including the associated appendices, click on <http://www.fema.gov/emergency/nims>.

The draft I2 guidance document can be accessed at the following website: <http://www.regulations.gov> under Docket ID FEMA-2008-0016. Public comments were accepted through 21 January 2009.

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

Is Your Membership About To Expire or Has Expired?

If YES, then visit www.DomesticPreparedness.com

Enter Promo Code: RENEW

to extend your subscription today!

Qualified members receive complimentary subscription

The Field Testing Dilemma and LRN Chemical Laboratories

By Richard France, Viewpoint



During a recent investigation of letters containing a white powder sent to a targeted company in several states, a common field detection device failed to identify the white powder. First responders used the device, known as the *HazMatID*, to try to identify the white powder from one of the letters in the field. Their instrument gave them a result that insinuated the presence of a non-toxic, inert chemical. Fortunately, the responders had enough white powder left to send a sample to a public health laboratory for testing.

The lab later identified the powder as a toxic chemical that could potentially cause illness if inhaled or ingested. The responders had learned a valuable lesson, and were fortunate that no one had been sickened by the white powder. The incident was a reminder to other first responders, though, to be constantly aware of the limitations of their own field-detection devices.

New Technologies: For Better or Worse

Over the last few years, first responders in the field have been placed in the difficult position of trying, with limited guidance, to identify various “unknown powders.” Further complicating the situation are the numerous new field instruments that promise to identify “unknowns” with the push of a button. On the chemical side alone, there are portable devices such as infrared and Raman spectrometers, photo-ionization detectors, and gas chromatograph/mass spectrometers. Many manufacturers tout their products as the absolute best in the identification of unknown chemicals,

but that assertion cannot be accepted without also considering under what conditions such statements hold true.

To begin with, a trained first responder must know beforehand what instrument to use and what it can and cannot identify. Not all authorities agree with the manufacturers’ statements about the versatility of certain field instruments. The Association of Public Health Laboratories’

**For almost
a decade the
LRN has been
responsible for
maintaining an
integrated network
of state and local
public-health,
federal, military,
and international
laboratories**

Statement of Position is that the association “*strongly opposes*” the use of biological and chemical agent detection kits and devices for field testing “*in the absence of performance standardization, field validation, and certified individuals trained in the application of these kits and devices* [emphasis added].” It is “essential,” the APHL Statement continued, “that a standardized validation, approval, and training process for these kits and devices be developed and implemented as soon as possible.”

Despite the association’s strong disclaimer, there is still no standardized validation process or established protocol governing the use of these field-detection devices. Moreover, sales personnel still make claims about their particular devices that have not been tested under laboratory conditions, let alone field conditions – and anecdotes abound about trained chemists working in a laboratory who cannot get this or that device to measure what the manufacturer claims it does.

Such problems present a difficult dilemma for first responders with a need to know about the efficacy of field testing for unknown chemicals. Fortunately, there is an independent organization – the Laboratory Response Network (LRN) – that can provide the guidance needed on these instruments. The LRN laboratories possessing a chemical testing/validation capability already are reaching out to the nation’s first responders, and to the health and medical communities in their own jurisdictions. In this way, they can become familiar with the first-responder process involving chemical-exposure incidents and determine how their own roles might complement response-and-recovery operations. The ultimate goal is the protection of the first responders themselves as well as anyone else coming into contact with suspicious substances.

The Anatomy of a Network

The LRN, which became operational in 1999, was established by the Department of Health and Human Services (HHS), working in

collaboration with the Federal Bureau of Investigation, the Centers for Disease Control and Prevention (CDC), and the Association of Public Health Laboratories. The mission of the LRN is to provide a nationwide coordinated laboratory response to bioterrorism, chemical terrorism, and other public health threats and emergencies. For almost a decade the LRN has been responsible for maintaining an integrated network of state and local public-health, federal, military, and international laboratories and, by doing so, enhancing the public health infrastructure by integrating the expertise and capacity of labs both nationwide and globally.

What are called the LRN-C (LRN Chemical) laboratories – which are headquartered at state public-health laboratories in cities across the nation – possess varying levels of capability. Currently, 62 state, territorial, and metropolitan public health laboratories participate in the LRN's chemical-detection tasks. A designation of Level 1, 2, or 3 defines the individual lab's LRN-C capabilities; each level builds upon the preceding level. All LRN-C members participate in Level 3 activities, which involve working with the health and medical communities, and first responders, in the collection, storage, packaging, and shipment of clinical specimens. All LRN-C members also work to develop a coordinated response plan for their state and geographical regions.

The laboratories designated as Level 1 or Level 2 are tasked with the analysis of clinical specimens to determine the presence of certain chemicals. Thirty-seven labs currently participate in Level 2 activities. These labs are trained to detect exposure to a limited number

of toxic chemical agents, such as cyanide or toxic metals present in human clinical specimens. Ten laboratories participate in Level 1 activities, and are trained to detect exposure to a greater number of chemicals such as mustard agents, nerve agents, and certain toxic industrial chemicals.

The LRN-C provides continuous support to its members, ensuring they are trained and proficient in the use of CDC-developed protocols and methods. These laboratories participate in a rigorous quality-assurance program to ensure that network labs provide precise, accurate, high-quality data. In a similar manner – and in an effort to work even more closely with their partners – many of the LRN-C laboratories are willing to help train or assess the proficiency of programs in which hand-held and/or portable instruments are used to identify unknown chemicals. This guidance is designed not only to assist first responders in the decision-making process but also to help them determine how much confidence to place in these devices.

Valuable Partners For First Responders

First responders obviously play a valuable role in coping with a chemical incident or “event.” They will, more often than not, be the first ones on the scene and will have to make a number of quick decisions about what they find. The goal of the LRN-C laboratories is to help the first responders make those decisions from a scientific point of view so that those at or close to the scene of the incident are safe.

There are two principal issues that must be addressed when deciding about using portable devices to

identify unknown contaminants in the field. The first is to consider how the results of the field test may change the incident response. If the confidence in the field screening is minimal then it is perhaps better to leave the instrument on the engine. One of the principal problems in field testing is that the chemical analysis could use up the entire sample – leaving nothing for a confirmation test later.

The second issue, which is probably even more important when unknown powders are involved, is the perception of a credible threat. It may be out of the individual responder's comfort zone to be required to identify what are, or are not, credible threats. That is when it may be advisable to bring in an FBI WMD (weapons of mass destruction) coordinator – and the LRN-C laboratories for consultation.

Those seeking the names of the laboratorians in the state public health laboratory nearest to them and the answers to questions about the Laboratory Response Network and/or the Association of Public Health Laboratories should contact Jennifer Beck at APHL (jennifer.beck@aphl.org).

Richard A. (Rick) France, a CT coordinator for the Florida Department of Health's Bureau of Laboratories, has been a Chemical Terrorist Laboratory Coordinator at the Bureau's Level 3 laboratory in Tampa since 2004; the Tampa laboratory is a part of the nationwide Laboratory Response Network. Level 3 CT coordinators are responsible for working not only with various federal, state, and local agencies in their jurisdiction but also with first responders and the health and medical communities to provide training and coordination on matters related to chemical terrorism preparedness and awareness.

Cold Calculations and the Search for Inner Warmth

By Joseph Cahill, EMS



With arctic air masses moving across the country this week, the issue of cold has moved to the forefront of many people's minds.

For EMS (Emergency Medical Services) agencies and organizations there are particular concerns about two groups of people – patients, and EMS crews.

Extreme cold puts added stress on patients who are already ill or injured, in ways not necessarily connected to the cold. Cold stress makes shock states worse, and for that reason extra steps must be taken to ensure patient warmth. Finally, in addition to these problems, which make the handling of the normal patient load that much more difficult, there are a number of additional patients whose principal or only medical problems are caused by the cold itself.

Isolated areas of skin exposed to extreme cold over a period of time can freeze, creating a condition, popularly known as frostbite, that is extremely damaging to the tissue involved. A greater danger is the lowering of body temperatures. The delicate chemical reactions that make up the human body can operate within only a limited range of temperatures. Exposure to the cold – *or exposure to any conditions that rob the body of its own natural warmth* – lowers the patient's body temperature; this condition is known as hypothermia, and is also extremely dangerous. As the body loses heat it eventually reaches the point where it shuts down completely.

Shivering in a Stand-by Status

The members of ambulance crews are of course just as susceptible to

the cold as anyone else. But there is an aggravating factor involved: During the course of their duties, EMS staff are often required to spend extended periods of time either in their vehicles or outside, waiting at an incident scene where they are exposed to the weather.

In many cities, ambulance crews are required to remain in their vehicles, usually parked on the street, when not on a specific assignment. These long periods of

**Warming a patient
“from the inside” is
the most medically
effective process to
follow, because the
human body starts
to shut down one
part at a time,
starting with the skin
and extremities**

time sitting in the ambulance can create major health problems if the heating in the cab is not sufficient to help the EMS staff maintain their own body temperatures. This problem is exacerbated by the fact that EMS crews are often called on to “stand by” at the scene of incidents (fires, for example) or mass gatherings – e.g., the recent New Year's Eve celebrations, and last week's Inaugural Parade in Washington, D.C. – even when EMS

is not the initial or principal focus of the gathering.

At a minimum, ambulance heating systems should be tested – and, if necessary, repaired – well in advance of winter weather. The same maintenance check-off list recommended for the family car should be used for emergency vehicles, paying particular attention to ensure that the coolant is checked and that the entire cooling system is flushed if needed. The check-up also should include a close examination of the exhaust systems; carbon monoxide buildup within the cab of a vehicle with tightly closed windows could be a significant hazard. Vehicles lacking a fully operational heating system should be taken out of service until they are repaired.

Blanket Protection, IVs, and Flexible Garments

During the winter months, additional blankets should be added to the equipment usually carried in each vehicle. Ideally, provisions also should be made to ensure that the recommended temperatures for intravenous (IV) fluids and oxygen can be maintained; warming a patient “from the inside” is the most medically effective process to follow, because the human body starts to shut down one part at a time, starting with the skin and extremities. In contrast, warming from the *outside* causes the cold blood that has been trapped in the extremities to return to the inner core of the body, thereby lowering the temperature of the inner core.

OUR MISSION YOUR SAFETY



SAFESITE® MULTI-THREAT DETECTION SYSTEM

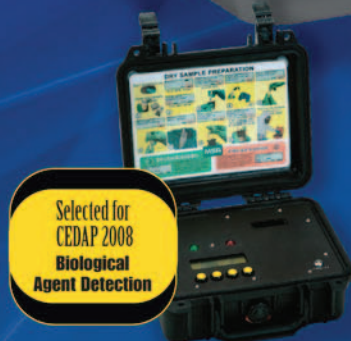
**Critical Infrastructure
Emergency Response
Public Events
Perimeter Monitoring**

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

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



**VISIT US ONLINE
MSANET.COM**



**BIOLOGICAL
AGENT DETECTION**



**CWA & TICs
HANDHELD PORTABLE**



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


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

Special care is required to ensure that EMS crews also are provided with outer garments that not only provide the warmth needed but also allow the flexibility to perform their work without significantly shedding those garments. A sometimes more important need – on the scene of an incident where an EMS crew may be kept waiting for a long period of time – is to ensure that there is adequate shelter from the elements.

With the radio communications now available in almost all political jurisdictions throughout the country it is unconscionable to force EMS staff (and/or other first responders) to simply “stand by” in the cold – or, during the summer months, in extreme heat – until they are actually needed. Stationing the EMS staff in the lobby of a nearby building, or in their own vehicles, until they are actually needed decreases the risks to their own health without decreasing their operational effectiveness.

The first responsibility of any emergency agency is to ensure the safety both of its own staff and of other responders directly involved in EMS operations. Preparation for the cold is vital not only for the safety of the crews themselves, but also for the survival rate of the patients they serve.

Joseph Cahill, a medicolegal investigator for the Massachusetts Office of the Chief Medical Examiner; previously served as exercise and training coordinator for the Massachusetts Department of Public Health, and prior to that was an emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as the citywide advanced life support (ALS) coordinator for the FDNY - Bureau of EMS, and prior to that was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem.



How the NDMS Can Be Made More Effective

By Michael Allswede, Public Health



“The art of progress is to preserve order amid change and change amid order.”

Alfred North Whitehead

Alfred North Whitehead was a physicist, mathematician, and philosopher who witnessed the demise of Newtonian physics and advance of Einstein's Theory of Relativity during the early 1900s. Whitehead was classically educated to believe that matter is unchanging and always constant, but he ultimately embraced the fundamental concept of relativity (that matter and energy may exchange) and helped usher in the nuclear age. His wisdom, cited above, on the art of progress may also help to guide the development of medical responses to meet future challenges in the era of terrorism.

Today, disaster medical response is undergoing fundamental shifts, primarily because of financial pressures, a long series of natural disasters, and the escalating threat posed by international terrorism. In years past, adequate disaster medical response could be reasonably expected to cope with the occasional weather emergency, some if not all natural disasters, or even a major industrial mishap in which a specific disaster area could be both determined and defined, after which resources could be gathered and lives would be saved. Although the loss of life is tragically inevitable during such events, in the past those events seldom had the capacity to destabilize the American way of life.

That is no longer true. Looking ahead to the potential disruptions that might be caused by such events in the future, it seems obvious that the American way of life may indeed be placed at much greater risk in the future, if only because of flaws and/or built-in weaknesses within the medical response system itself. Today, for example:

- Because of financial pressures, most state and local medical systems have much less excess capacity than in years past;
- The U.S. population is not only growing older but also becoming ever more dependent upon outpatient services – which are *not* a built-in component of the nation's disaster medical service capabilities; and
- Certain future disasters, particularly terrorist incidents, pose a greater threat than in the past, if only because of the need for detection and characterization of such incidents before an effective response can be mounted.

Definitions, Descriptions, And Determinations

For all of those reasons, and to plan the stockpiling of the resources needed to deal with the *next* crisis (rather than the last one – i.e., the one most recently encountered), it may be useful to divide disasters into two principal subtypes: “overt,” and “covert.” An overt disaster could be described as one that is both recognizable and definable – e.g., a bombing, a flood, or a hazmat (hazardous materials) event. There would be a defined *start* to such an event, a defined *geography* (i.e., the area where the

event occurs and is limited to), and a defined *population at risk*. Each type of overt disaster could then be characterized by victim injury patterns, and the resources needed to cope with it could be logically estimated and planned.

A key factor in the development of such estimates, obviously, would be a thorough understanding of perhaps the most critical component of the estimate: the relevant response time involved. Each specific type of disaster is usually characterized by a recognizable “velocity” of victim deaths – most of which, in most incidents, would occur in the first 24 hours following the start and/or initial recognition of the disaster. To be a *useful* resource, however, such estimates must be available within a relevant timeframe. Obviously, it does little good to have the world’s best equipped decontamination facility available 24 hours after all victims have either died or fled a hazmat scene.

What is called the National Disaster Medical System (NDMS), a major agency of the U.S. Department of Health and Human Services (HHS), was developed specifically to provide an effective response to overt disasters. The NDMS is composed of: (1) a deployable response arm, consisting of volunteer teams such as the 54 Disaster Medical Assistance Teams (DMATs) strategically positioned throughout the country; and (2) a nationwide network of NDMS hospitals. The latter, originally intended to serve as excess capacity for the Veterans Administration hospital system in time of war, are expected to make at least part of their existing capacity available for the care of disaster victims. But that may not always be possible – for a number of understandable reasons.

Unfortunately, because the NDMS is based primarily on volunteerism, the system lacks both rapid-response and sustained-response capabilities. The reality is that most of the working professionals on the NDMS roster not only must extricate themselves from their “regular day” duties but also, in most situations, would be limited in the duration of their


**The NDMS
did not play a
significant role
either during the
anthrax events of
2001-02
or in the less
publicized responses
to more recent
infectious-disease
events**

deployments. To cite but one example: Of the approximately 200,000 medical evacuations carried out during Hurricane Katrina, only about one percent were carried out by NDMS agencies and personnel. Because of the inherent limitations of almost any volunteer system, in fact, most of the disaster care during and after not only Hurricane Katrina but also after the bombing of the Murrah Building in Oklahoma City and the 11 September 2001 terrorist attacks in New York City and Washington, D.C., was provided by local medical agencies and assets, not by the NDMS.

Fundamental Differences And Other Complications

Covert disasters – e.g., an infectious disease epidemic, food or water contamination, or bioterrorism – create a fundamentally different order of priorities. Because a covert event will, in most cases, initially seem to be some type of illness, the nature of the disaster must first be recognized by the local medical system, then officially characterized (particularly in the case of a bioterrorism event) by a local public-health and/or law-enforcement investigator before a *national* response can be ordered. Because such illnesses will progress steadily – and sometimes very rapidly – until containment is achieved, the medical response to victims must proceed *concurrently* with the investigation. Complexities such as a patient’s right to medical privacy, the constitutional law protections mandated for potential criminals, and the duties and responsibilities assigned to a national command authority can be expected to impede the investigation of ill victims who also may be witnesses to a bioterrorism event – and/or, in certain cases, even create difficulties in investigating the terrorists themselves.

There are other complications that must be considered in determining if and when a *national* disaster medical response may be needed. One such complication is that there are at present either no NDMS assets available for toxicology, infectious disease, or radiation health, or such assets are available in very small quantities. It is largely for that reason, in fact, that the NDMS did not play a significant role either during the anthrax events of 2001-02 or in the less publicized responses to other, more recent, infectious-disease events. Moreover,



instead of developing a cadre of trained personnel to deal with covert-event response contingencies, the federal government has instead paid much greater attention to the development of a Strategic National Stockpile (SNS) of the medicines and equipment needed to support existing medical facilities throughout the United States.

Unfortunately, the little-known secret in coping with covert events is that communicable diseases and/or contamination usually will create secondary victims within the local medical and other healthcare facilities mobilized to cope with such events. In addition, at least some – and perhaps quite a few – local medical and allied support personnel may not report to work during a communicable-disease or contamination event because their own first priority may be to save themselves and/or their families. By not providing trained personnel as well as the SNS assets, the federal government has made it possible for a covert event to thwart the SNS strategy through reductions in the local work force.

The Dual-Assignment Path to A Double-Jeopardy Dilemma

The threat of terrorism further complicates the issue of NDMS response, if only because overt events such as the recent bombings in Mumbai are planned by and under the control of America-hating fanatics who have the habit of repeating successful attacks until they are stopped. Because of their volunteer status, DMAT members may defer deployment in anticipation of a future attack on or within their own communities. Moreover, many DMAT members

also have affiliations with state and local response teams. Although well intended, such dual assignments would obviously create a “double jeopardy” situation for response personnel. For similar reasons, such covert events as the outbreak of a communicable disease could be expected to degrade or defeat outright the volunteerism component of the DMAT strategy. In short, although most U.S. medical providers – doctors, nurses, emergency medical technicians, ambulance drivers, etc. – are generally receptive to voluntary service, an undetermined but perhaps rather large number can be expected to want to serve their own communities first during a time of widespread crisis.


Given the need to fight the next war, not the last one, it seems clear that the NDMS must evolve from its current system of generic volunteer medical teams into more relevant units – possessing a broad spectrum of specialty skills, and available for rapid deployment. The challenge here is to promote such an evolution while preserving the stronger elements of the current system. A potential methodology for this process could start by: (a) taking a much closer look at the 15 situations that the Department of Homeland Security (DHS) has described as the “most likely” scenarios for future terrorist attacks; and (b) calculating the medical assets needed and the relevant response times related to each of those scenarios. By developing both a list of the resource needs and the probable time frames available for the primary set of homeland security threats, a more accurate determination can be made as to

whether a given asset should remain in the current NDMS organization, or perhaps be distributed to state or local teams.

Special attention also would have to be given to the detection assets and strategies needed to cope with covert events. Because such events would almost always first be detected locally, augmenting university medical centers, trauma centers, and/or poison centers to develop and maintain an effective response capacity would be another high-priority concern. By investing in the nation’s existing medical system to develop the capabilities needed for a true national disaster medical response system, the existing U.S. healthcare system may also become part of the NDMS.

These and other remedial actions would necessarily require a rather large investment of taxpayer dollars – always difficult, but even more so during and because of the current economic crisis. However, the cost of *not* evolving the current NDMS into a larger and more comprehensive – as well as more effective – organization specifically designed to meet the most likely future challenges is that the victims of the next disaster may be waiting for a non-existent or poorly designed “cavalry” to come over the hill to their rescue. And the cost of waiting would be paid not only in dollars, but also in lives lost that might otherwise have been saved.

Dr. Michael Allswede is the Director of the Strategic Medical Intelligence Project on forensic epidemiology. He is the creator of the RaPiD-T Program and of the Pittsburgh Matrix Program for hospital training and preparedness. He has served on a number of expert national and international groups on preparedness.



No Time to Cut Back on Safety – The Cost Is Too High

By Warren K. Brown, Building Protection



Workplace safety processes must be in place at all times and are even more critical during business downturns – if only to prepare for unexpected incidents and prevent worker injuries, illnesses, or even death. Companies that have a strong safety culture and continually invest in and implement effective safety processes see positive results, including a reduction in worker injuries and illnesses as well as a parallel reduction of costs associated with injuries to employees – e.g., worker's compensation payments and time lost from work.

During financially difficult times, cutting costs by reducing safety ultimately hurts businesses, leaving them unprepared for unexpected incidents that end up costing them more in the long run. Businesses spend an estimated \$170 billion a year on costs associated with workplace injuries and illnesses, and pay almost \$1 billion every week to injured employees and their medical providers. In addition, when companies do not invest in safety they may face a damaged reputation and brand when employees are injured, especially if the incidents are or were preventable.

Investing in safety pays off in many ways and contributes positively to a company's bottom line. For example, a recent study of an investment firm in Australia showed clear links between workplace safety and health factors and investment performance. The results of the study indicated that companies that did not adequately manage workplace-safety issues did not perform as well financially as companies that did pay greater attention to safety.

Prudent and Practical Preventive Measures

Although most companies are always looking for ways to cut costs, even and perhaps particularly in the current very difficult economic climate, they should not forget that there are many ways to save money without cutting corners on business safety measures and programs. The South Carolina chapter of the American Society of Safety Engineers (ASSE) has suggested that employees can take a number of prudent and easy-to-implement measures to help companies save money without compromising safety and health in the workplace. Among the most important, and most obvious, of those measures are: (a) following safe working procedures and practices to not only prevent injuries but also to reduce related downtime and expenses such as costly fines; (b) properly using, cleaning, and caring for personal protective equipment (PPE); (c) re-using gloves whenever possible – and for as long as possible; and (d) keeping track of safety glasses and re-usable hearing devices and equipment.

Laura Comstock, president-elect of ASSE's South Carolina chapter, emphasized that when safety-related items – e.g., employee PPE such as hardhats, safety glasses, and respirators – are critical to operations their purchase must not be deferred. Safety training during tough economic times also should not be deferred, she added, pointing out that some safety-related training is time-sensitive and therefore cannot and should not be delayed. She also suggested, though, as an alternative, that some training costs can be reduced by using online or electronic-based training services

instead of requiring face-to-face settings in a classroom for safety training. In addition, having on-site safety and training professionals available at the workplace reduces costs by allowing training to take place both on-shift and at jobsites, thereby eliminating the need for overtime sessions and/or taking employees off the job for extended periods of time.

Accidents and incidents will still happen, of course, but companies that continue to invest in safety – and, of perhaps even greater importance, that create and maintain a safety *culture* – will almost always reduce the number of injuries and illnesses associated with unexpected events at the workplace and/or during working hours. When incidents do occur, those same companies should and will have in place the tools needed to protect people, property, and the overall work environment.

In short, establishing and maintaining a comprehensive safety program continues to be essential for business operations not only now, during difficult economic times, but at all times, not only to prevent unnecessary tragedies – the most important objective – but also to reduce normal everyday operating expenses. The bottom line, employee and customer *safety*, is good business, always.

Warren K. Brown is safety supervisor of DMAX Ltd. of Moraine, Ohio. He also is a 30-year member, and current president, of the American Society of Safety Engineers. Prior to affiliating with DMAX he served as a plant layout engineer, OSHA coordinator, and both supervisor of safety and associate administrator of safety for General Motors and Delphi. A certified safety and health manager, he has won a number of national awards in the field of industrial safety. ▼

California, Ohio, Kansas, and Louisiana

By Adam McLaughlin, State Homeland News



California **Overworked Hospitals** **Under Heavy Stress**

It is not a Friday night, or even the peak of flu season. It is a normal weekday afternoon at the County Harbor-UCLA Medical Center, a facility near Torrance that treats some of the county's poorest and sickest patients. Nonetheless, the average wait here – depending on the severity of a patient's injury or illness – is about eight hours. The problem is neither financial nor political, but simply the result of an overburdened hospital system the capacity of which has been stretched thin.

The recent domino effect of hospital closures and bed reductions – four hospitals have closed in the South Bay area, 10 emergency rooms in the county also have shut down, and at least two other hospitals have reduced bed capacity – has left many healthcare experts worried that the increasingly fragile network will not be able to cope with a major event resulting in a massive number of casualties. That event could be anything from a natural disaster or terrorist attack to a freeway pile-up, the outbreak of a pandemic flu, or a plane crash.

“If Southern California's hospitals cannot handle patient inflow even during the course of a normal day, I have grave doubts about how the region would do in a disaster scenario,” said James Lott, executive director of the Hospital Association of Southern California, a trade group. “Any increase in demand would stretch the system beyond what it could handle.”

Los Angeles County as a whole has a meager 1,500 “excess” beds on any given day, according to a 2007 study by Price Waterhouse Cooper, a nationally known consulting firm. More than half of all of the area's hospitals are “on diversion” – meaning they have to turn away ambulances because they are already too crowded – at least 20 percent of the time. The numbers are worse for highly specialized facilities. Three-quarters of the teaching hospitals in the area – Harbor-UCLA, for example – are either at or over capacity in their emergency department at any given time, according to the 2007 study.

Harbor-UCLA, on Carson Street in an unincorporated area between Harbor Gateway and Carson, is almost literally bursting at the seams. A 2008 survey, carried out from January to May of last year by the California Department of Health Services (which runs the hospital), showed that, when the hospital is operating at optimum capacity, even a slight patient surge of 5 percent or so pushed waiting times to over 14 hours. State inspectors cited and fined the hospital twice last year for lapses in care; one of the incidents cited was a direct result of emergency room crowding.

In a major disaster such as an earthquake or a terrorist attack the normal rules for care – nurse-to-patient ratios, for example – although not ignored, may be impossible to follow, according to Dr. Roger Lewis, an emergency-room physician at Harbor-UCLA (and a professor in the Department of Emergency Medicine). “When you're talking about hundreds of victims, you are operating with a different mind-set,” he commented.

But it may be the smaller, longer-lasting disasters, such as a worse-than-average flu season, that cause greater hardships not only for patients but also for medical personnel, said Lewis, who has written extensively about surge-capacity problems. “Surge is not just about a shortage of physical beds,” he said. “You are also talking about a shortage of [the] staff needed” to care for the additional patients.

Ohio **Emergency Radio System** **Passes Initial Tests**

Butler County's new emergency communications radio system has been successfully tested at more than 2,000 locations across the county, according to project manager Matt Franke, who said that, despite some earlier delays, the county would be ready to flip the switch on the new \$35 million system in early 2009. First, though, emergency responders will be trained on the system (in January), and roughly 2,200 handsets will be distributed.

Franke said the system worked acceptably at the spot where Butler County Sheriff's Deputy Brandon Roberts was nearly killed in a 2005 shooting – a time when emergency responders had to relay messages through cell phones. Once the new radio system is operational, said Sheriff Richard K. Jones, “We will not have to use cell phones ... [to talk to] the different jurisdictions. ... There were spots back then [in 2005] when you couldn't even communicate with each other.”

More recently (on 14 September), Franke said, the system “operated flawlessly” – even though few jurisdictions were equipped with it – after power had been knocked out countywide by a windstorm. The

unexpected outage “ended up being a good test for us,” he said. “It showed [that] everything worked.”

After this month’s training sessions have been completed, the county’s 21 fire departments and 14 police departments will start coming on line one at a time, a process that could take several months. To prevent confusion, Franke said, local fire stations have had to rename some of

their vehicles so there would be no misunderstanding if someone talked about “engine five,” for example.

In addition to being able to operate even in remote parts of the county, Jones said the system’s 800-megahertz signal strength will allow emergency responders to communicate from inside thick-walled buildings. The inability to do this was a shortcoming that

proved fatal to a number of New York City firefighters at the time of the 11 September 2001 terrorist attacks. “Sometimes, when the ... [NYC firefighters] would go into buildings,” Jones said, recalling that situation, “they would have no communication whatsoever.”

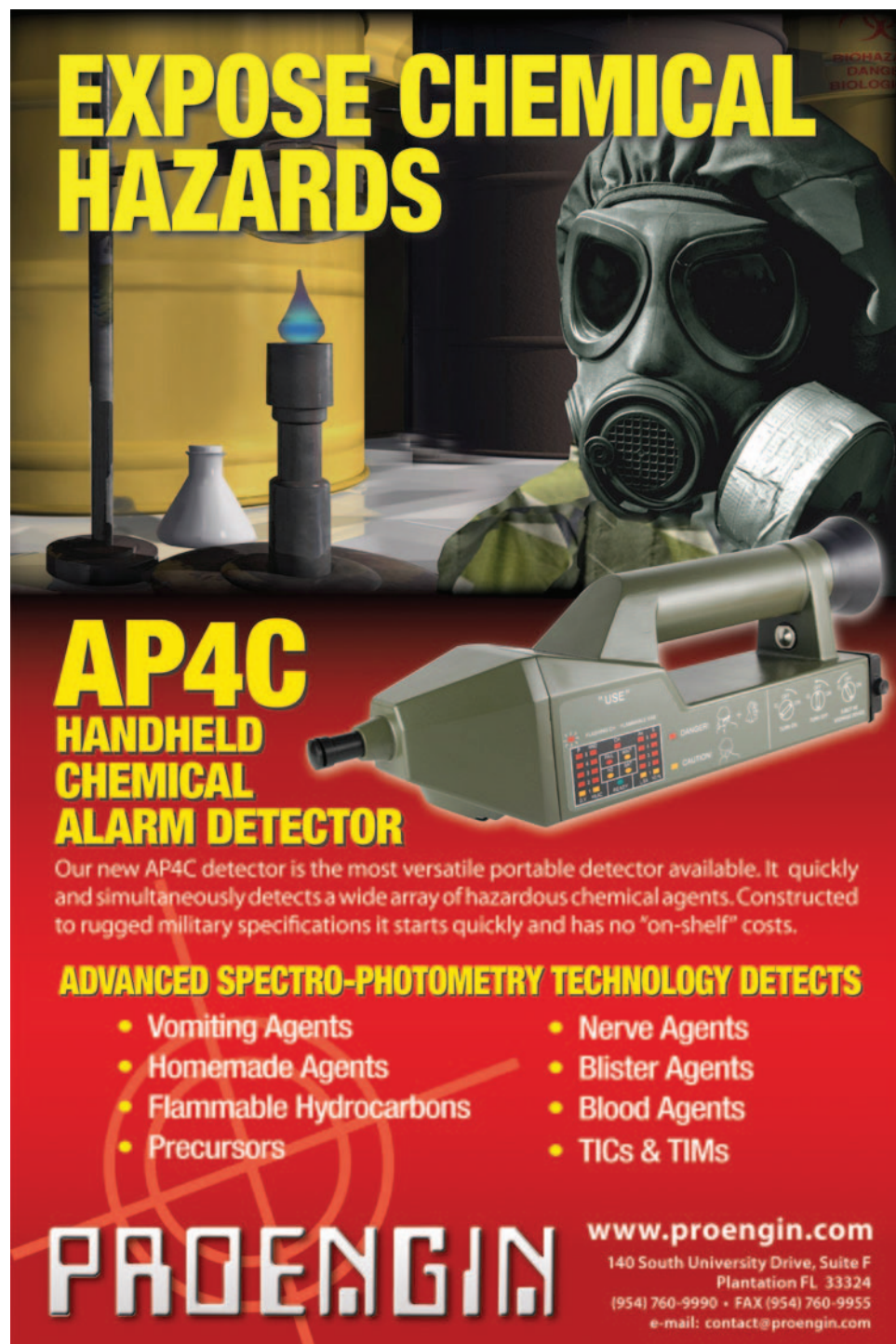
Franke listed several other benefits provided by installation of the new system: fewer garbled signals, for example, and the ability for different jurisdictions to communicate directly with one another. By using the new system, he said, “A salt truck driver in West Chester could talk to an animal control officer in Oxford.”

Kansas

Manhattan Will Be Home To National Bio & Agro-Defense Facility

The Department of Homeland Security (DHS) has announced the selection of Manhattan, Kansas, to be the site of the new National Bio and Agro-Defense Facility (NBAF). U.S. Senator Pat Roberts (R-Kan.) said the decision to locate the new \$650 million federal animal and plant disease laboratory on the Kansas State University (KSU) campus represents “one of the most significant investments to the Kansas economy in state history.”

The NBAF will replace the aging Plum Island facility in New York. The research conducted by NBAF will be designed to find new ways of protecting animals, food crops, and consumers from disease threats. The new center will research high-consequence biological threats involving foreign animal diseases as well as those classified as zoonotic – i.e., capable of being transmitted from animals to humans. Its operational charter calls for, among other tasks: basic research; diagnostic development, testing, and validation; advanced



EXPOSE CHEMICAL HAZARDS

AP4C HANDHELD CHEMICAL ALARM DETECTOR

Our new AP4C detector is the most versatile portable detector available. It quickly and simultaneously detects a wide array of hazardous chemical agents. Constructed to rugged military specifications it starts quickly and has no “on-shelf” costs.

ADVANCED SPECTRO-PHOTOMETRY TECHNOLOGY DETECTS

- Vomiting Agents
- Homemade Agents
- Flammable Hydrocarbons
- Precursors
- Nerve Agents
- Blister Agents
- Blood Agents
- TICs & TIMs

PROENGINE

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

countermeasures development; and training for high-consequence livestock diseases.

The new federal bio-containment will also:

- Assess and research bioterrorism threats evolving over the next five decades;
- Enable the U.S. Departments of Homeland Security and Agriculture to fulfill their related homeland defense research, development, test, and evaluation (RDT&E) responsibilities; and
- Integrate those aspects of public and animal health research that have been determined to be essential to national security.

The KSU site was selected over potential sites in four other states. Roberts attributed the state's success in attracting the facility to a collective effort that including the state government, a special NBAF task force, the Kansas Bioscience Authority, and senior officials at KSU and the city of Manhattan. "We can really be proud of our teamwork to prove that Kansas is the best home for this laboratory based on the merits," said Roberts.

Louisiana

New Orleans to Receive \$4 Billion In New Post-Katrina Contracts

The Army Corps of Engineers plans to award more than \$4 billion in new post-Katrina contracts this year for construction of new levees and additional drainage projects that should make the entire coastal region safer and provide a major economic boost to the local economy.

"The 113 contracts for the hurricane and storm-damage risk-reduction

system will be the largest number we award in any given year," said Army Corps of Engineers Col. Gregory Gunter. In addition to the \$4 billion in new flood-protection contracts – all for the greater New Orleans area – several other federal and state coastal-restoration projects costing close to \$1 billion are expected to start construction later this year.

**Research conducted
by the NBAF
will be designed
to find new ways of
protecting animals,
food crops, and
consumers from
disease threats**

The new contracts represent a major additional allocation for the multi-year effort to build a flood-protection system capable of protecting against so-called "100-year" storms – which are defined as particularly dangerous hurricanes that have a 1-in-100 chance of making landfall during any given year. The corps expects to meet its goal of providing a 100-year level of protection by 2011.

The new round of contracts – combined with earlier contracts for initial repairs to the levee system so heavily damaged by Hurricane Katrina, and for improvements to the area's interior drainage system – brings to almost \$15 billion the total funding that, when the last projects are completed in 2013, will have been spent in the area to prevent a Katrina repeat.

Meanwhile, longer-range plans for providing protection from 400- or

even 1,000-year storms – similar to or stronger than Hurricane Katrina itself – remain in a holding pattern. The Corps of Engineers has missed several deadlines for providing recommendations to Congress for providing the higher level of protection, commonly called "Category 5" protection, but has promised to deliver a more definitive report by June of this year.

This biggest contract expected to be awarded this year – to finance a new gate complex to block storm surges from entering the Harvey and Algiers canals – is expected to cost more than \$500 million. That project is not expected to be completed until 2013.

Several other contracts, estimated to collectively cost more than \$100 million, will raise hurricane-protection structures surrounding St. Bernard Parish to similar 100-year levels. The corps has reduced the cost of those projects somewhat by planning to build sturdy floodwalls, shaped like an upside-down T, atop earthen levees in most of the areas covered; the floodwalls will significantly reduce the amount of land needed to build the higher structures, Gunter said. The floodwalls will be "a change in what they are used to seeing out there, which is a clay levee," Gunter said. "It [building of the floodwalls] will be a more economical alignment. But that is really in terms of the cost of the additional real estate that would be required, should a traditional levee ... [cave] in."

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



THE INSIGHT TO SECURE OUR NATION

GovSec and U.S. Law: the one place to see and experience it all! From a solutions-based Conference, insightful Briefings, expert Keynotes, a host of Special Features, and Exhibitors offering cutting-edge security products, no other event offers such a comprehensive approach to securing our country and ensuring the public safety.

All that expertise is translated into action right on the exhibit floor where you'll see, touch, and test solutions that turn theory into reality. Products include:

- Access Control Systems
- Biometric Control Systems
- CBRNE Detection & Mitigation
- Data & Voice Communications
- Disaster Preparedness & Recovery
- Intrusion Detection
- IT Security & Software
- Lethal and Less-Lethal Weapons
- Military Equipment
- Mobile Command Centers
- Perimeter Security
- Personal Protection Equipment
- RFID Systems
- Specialty & Security Services
- Surveillance Systems
- Tactical Products
- Training & Education
- ... AND MUCH MORE!

As an added bonus, your registration will admit you to FOSE, which is co-locating with GovSec and U.S. Law. You and your colleagues will be immersed in the convergence of IT and physical security, expanding your arsenal of tools for accomplishing your mission.

Products. Strategies. Tactics. Education. Networking.

Join your colleagues from this focused and highly qualified community at GovSec and U.S. Law.

Register today for COMPLIMENTARY* expo admission.

MARCH 11-12, 2009

**Walter E. Washington Convention Center
WASHINGTON, DC**

www.govsecinfo.com

Produced by:



**1105 GOVERNMENT
Information Group**

Questions, or to exhibit — contact us today:
govsec@1105govinfo.com or 800.746.0099.