

An Endangered World Running Out of Time?



- ▼ Scenario: Pakistan Falls to Taliban
Neil C. Livingstone, Viewpoint
- ▼ Preparing for Worst in Cyber Security
Amit Yoran, Cyber & IT Security
- ▼ Beslan School Massacre
A Threat with No Easy Solutions
Patrick Bird & Michael Allswede, Law Enforcement
- ▼ Isolation, Quarantine, & Time
Joseph Cahill, EMS
- ▼ Field Testing or LRN Laboratories?
Rob Schnepf, Fire/HazMat
- ▼ The Future of LPR Technology
Rodrigo (Roddy) Moscoso, Law Enforcement
- ▼ Today's Well-Suited Responder
Glen Rudner, Fire/HazMat
- ▼ Mass Prophylaxis:
The Brass Ring of Public Health
Bruce Clements, Public Health
- ▼ A Spring of Tragedy
Joseph Trindal, Law Enforcement
- ▼ Massachusetts, California,
Montana, and New York
Adam McLaughlin, State Homeland News

innovative technology solutions.

A black and white photograph of emergency responders in full gear, including helmets and oxygen tanks, carrying a stretcher with a patient. The scene is dynamic and slightly blurred, suggesting movement in a high-stress environment.

**scalable.
mobile.
robust.**

irms

The premier homeland security COTS application

Emergency, Resource,
Patient, Clinic, Asset and
Warehouse Management

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

Staff

Martin Masiuk
Publisher
mmasiuk@domprep.com

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

John Morton
Strategic Advisor
jmorton@domprep.com

Dan Brethauer
Account Executive
dbrethauer@domprep.com

Susan Collins
Creative Director
scollins@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

Advertisers in This Issue:

Bruker Detection

Idaho Technology Inc.

Knowledge Foundation - Biodetection
Technologies Conference

MSA

PROENGIN Inc.

Remploy Frontline

UFP

© 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 Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher.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.



Publisher's Message

By Martin (Marty) Masiuk



On 25 June 1950, North Korea launched a surprise attack against South Korea, starting a war that lasted more than three years and caused hundreds of thousands of casualties, many of them American. The war ended with an uneasy “truce” on 27 July 1953 with the establishment of an artificial and frequently violated demilitarized zone between North Korea and South Korea.


Earlier this week, Pyongyang struck again – with the UN-banned underground explosion of a nuclear device, the test-launch of five short-range missiles into international waters off the east coast of North Korea, and a steadily escalating barrage of violent threats against South Korea, the United States, and the United Nations.

The emerging possibility that a second and much more devastating Korean War might break out at any time was a serious distraction for U.S. and allied political leaders and military planners, who already were in the process of developing highly uncertain contingency plans on what to do: (a) when, and/or if, the Afghanistan-based Taliban should defeat Pakistan (and thereby acquire already operational nuclear weapons); and/or (b) Iran should continue its nuclear “enrichment” and “research” programs and also become a nuclear power to reckon with.

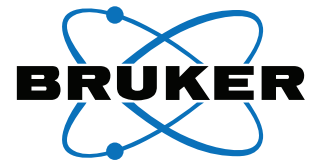
There is, of course, no totally effective way for the United States, acting on its own, or even with its allies, to deal with any of these suddenly major threats – or several others that might easily be imagined. But it is reasonable to suggest that the United States itself should and must focus much more attention on *total preparedness*, both at home and overseas, for the foreseeable future. Overseas, through the continued upgrading of the nation’s naval and military forces; and at home to cope with the still shocking reality that U.S. cities are now, for the first time since the War of 1812, vulnerable to enemy attacks – particularly attacks by domestic or foreign terrorist groups.

This month’s printable issue of *DPJ* deals in much greater detail with several of the nightmare scenarios mentioned above. Neil Livingstone’s leadoff article, in fact, describes the possibility of a Taliban victory in Pakistan as probably the single most dangerous scenario facing U.S. contingency planners. Two articles, by Bruce Clements and Rob Schnepf, deal with separate aspects of large-scale biological incidents, natural or manmade. Amit Yoran contributes an insightful analysis of a less bloody but economically devastating cyber-security invasion/intrusion. And Glen Rudner provides a helpful and somewhat more hopeful report on recent upgrades in the personal protective clothing and equipment items now available to help first responders cope with chemical and/or biological incidents.

Other domestic threats are covered by: Joseph Trindal, who comments on several nationally publicized shooting incidents that have both alarmed and energized the nation’s law-enforcement community; Joseph Cahill, who analyzes the national and global implications of the swine-flu outbreak earlier this year; Patrick Bird and Michael Allswede, who take a long second look at the Beslan School Massacre – and warn that the United States is not prepared to cope with a similar attack; and Rodrigo Moscoso, who provides an encouraging report on the many new crime-busting advances made possible by improvements in LPR (License Plate Reader) technology.

Rounding out the issue, as always, are timely reports, by Adam McLaughlin, on recent homeland-security upgrades, improvements, and advances in four states (California, Massachusetts, Montana, and New York) in different areas of the country. 

About the Cover: Studio shot, by Chad Baker, Getty Images, of an hourglass, with a globe inside, seeming to hover in midair.



Bruker Detection Corporation



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

E²M GC/MS System



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

HAWK FR Stand Off Detection



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

M-IR Mobile FT-IR



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

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

think forward

CBRN Detection

DomPrep Channel Masters

First Responders

Glen Rudner
Fire/HazMat

Stephen Grainer
Fire/HazMat

Rob Schnepf
Fire/HazMat

Joseph Cahill
EMS

Kay Goss
Emergency Management

Joseph Watson
Law Enforcement

Joseph Trindal
Law Enforcement

Rodrigo (Roddy) Moscoso
Law Enforcement

Medical Support

Theodore (Ted) Tully
Health Systems

Michael Allswede
Public Health

Raphael Barishansky
Public Health

Updates

Adam McLaughlin
State Homeland News

Viewpoint

Neil Livingstone
ExecutiveAction

Funding & Regulations

Diana Hopkins
Standards

Borders & Ports

Corey Ranslem
Coast Guard

Military Support

Jonathan Dodson
National Guard

"What Will It Mean for U.S. Domestic Security?"

Worst-Case Scenario:

Pakistan Falls to the Taliban

By Neil C. Livingstone, Viewpoint



The most significant and potentially devastating national-security threat now facing the United States, and the Obama Administration, would be the fall of Pakistan, a nuclear power, to Islamic extremists allied to Al Qaeda and the Taliban. Earlier this month the Taliban was within sixty miles of the capital of Islamabad and already engaged in fierce fighting with the central government, headed by President Asif Ali Zadari.

The Pakistani government, in a move roundly criticized in the West, had earlier negotiated a truce with the Taliban in the Swat Valley, once a tourist Mecca. In exchange for supposedly laying down their arms, the Taliban was permitted to impose Islamic, or sharia, law, on the region. But the Taliban reneged on their promise to disarm and instead introduced a reign of terror throughout the area, cutting off heads, burning down girls' schools, requiring men to grow beards and women to be fully covered, and mandating that disputes be settled in religious courts dominated by clerics rather than in traditional (i.e., slow and bureaucratic) secular courts.

Despite some encouraging Pakistani combat successes in the first two weeks of May, there was no guarantee that the Taliban advance could and would be stopped on a permanent basis. If the Zadari regime should collapse and be replaced by a Taliban-style government – such as the one that dominated Afghanistan prior to the U.S. intervention following the 9/11 attacks – President Obama and

his principal advisors would have to very quickly, and correctly, determine what that cataclysmic change would mean to security planners, law-enforcement agencies, first responders, and others tasked with protecting the United States itself.

A Potential Nuclear Holocaust?

The first and foremost question to be considered must be what would or could be done about Pakistan's nuclear weapons. If they are not secured by the United States and/or other nations and fall under control of the Taliban, the United States would, for the first time since the fall of the Soviet Union, face the real prospect of a nuclear attack, either against U.S. forces in the region or by a weapon surreptitiously slipped into the United States itself and detonated in one of America's great cities. The Taliban might well share its nuclear arsenal and technology with other rogue nations, or even with terrorist groups such as Al Qaeda, immensely compounding the threat.

Another nightmare possibility is that other nations might find the threat of a nuclear attack from Pakistan or its allies so terrifying that they would decide to take preemptive action on their own, igniting a regional war that could quickly become a global conflagration. There already have been credible reports that Israel and India, to take but two likely examples, have been meeting secretly to develop a joint contingency plan to take out the Pakistani nukes if extremists seize power in Islamabad.

In addition to preparing to cope with potential nuclear threats, U.S. law-

enforcement agencies and others involved in homeland security would have to anticipate a potential wave of terrorism that could dwarf the consequences of the 9/11 terrorist attacks. In order to fend off external challenges, an extremist government in Pakistan could be expected to unleash terrorists throughout the world, providing them with safe haven, training, explosives, and logistics support.

A Flood of Refugees And a Major Language Problem

The imposition of a Taliban-style government on Pakistan might also create one of the largest floods of refugees in modern times, with millions of homeless Pakistanis seeking safe haven in other countries in the region – or in the West. This would produce a humanitarian crisis of epic proportions and create a huge problem for countries taking in refugees as they attempt to sort out the terrorists and sleeper agents from the bona fide human victims fleeing Taliban oppression.

The United States would be a favored safe haven for many of the refugees. There are currently an estimated 300,000 to 500,000 people of Pakistani origin in this country, about half of them already U.S. citizens. The largest concentration is in the New York City area; other large concentrations are in Houston, Chicago, and Washington, D.C. – and all of those communities would serve as natural magnets for both legitimate refugees and terrorist sleeper cells.

An Islamist victory could be expected to raise the U.S. homeland-defense threat to its highest level since 9/11, triggering tightened security at airports, seaports, military installations, public buildings, and elsewhere throughout the country. To prepare for that scenario, U.S.

federal, state, and local intelligence agencies would have to significantly build up their intelligence sources, including informers, in the U.S. Pakistani community. This would be a difficult enough task in itself, but it would be compounded exponentially by the fact that there are very few U.S. intelligence personnel fluent in Urdu, the official language of Pakistan – and/or in several other languages (including Punjabi, Pashto, Balochi, Sindhi, and Saraiki) spoken in Pakistan, along with countless dialects. Most U.S. law-enforcement and intelligence operational personnel also suffer from a major deficit in terms of their knowledge of Pakistani culture, customs, and etiquette.

The real challenge for U.S. policymakers now is to shore up the Zadari government and to provide it with the money, training, and materiel resources needed to defeat the Taliban and reassert Islamabad's control over the northwest border

reaches of Waziristan – where, not incidentally, Osama bin Laden and his closest followers are believed to be hunkered down.

For President Obama and his principal advisors, the most important point to remember is that, if the war against the Taliban can be successfully waged in Pakistan, it will not have to be fought in the continental United States itself. As President Zadari pointed out less than two weeks ago (on 7 May), to an audience that included the U.S. Joint Chiefs of Staff and CIA Director Leon Panetta, “We are all in this together, and our fates are inextricably linked.”

Dr. Neil C. Livingstone, chairman and CEO of Executive Action LLC and an internationally respected expert in terrorism and counterterrorism, homeland defense, foreign policy, and national security, has written nine books and more than 200 articles in those fields. A gifted speaker as well as writer, he has made more than 1300 television appearances, delivered over 500 speeches both in the United States and overseas, and testified before Congress on numerous occasions. ▼

Keeping Water Facilities Safe

Webinar to address the role of law enforcement in protecting the nation's drinking water and wastewater infrastructure.

Topics Will Include:

- Threats & vulnerabilities related to the water sector
- Role of law enforcement agencies in responding to a water emergency
- Components of drinking water & wastewater systems
- Additional sources of information on protecting the water supply

In the Briefing Room
FREE with Registration



Sponsored by



Preparing for the Worst in Cyber Security

By Amit Yoran, Cyber & IT Security



To most preparedness and emergency-response professionals, effective planning is essential to the execution of every mission.

Their organizational mandate is wide in scope and incredibly complex, but relatively simple at its core: Imagine the worst possible scenarios and take them into account to ensure that the organization's readiness to respond is not diminished in the unlikely event any of those scenarios occur.

This is particularly true if the organization has a vital role to play in the protection of national health and human life. Whether the scenario postulated is a natural disaster, a pandemic outbreak, riot control, or an act of domestic or international terrorism, the organization or agency should have very carefully – and in advance – developed, documented, and tested its response plans.

Even if all this is done, though, there still might be one critical type of “unnatural” disaster scenario that many emergency-response professionals have not considered thoroughly: a failure to protect the organization's own IT (information technology) security strategy and its resilience to cyber attacks. This oversight could easily jeopardize the organization's ability to respond effectively.

Trojan Horses Vs. Imperfect Science

Because of the importance of IT systems, many organizations in the preparedness and emergency-response field are ideal targets for cyber attacks. The information managed and used by these organizations is of immeasurable value for a number of potentially

harmful purposes. State-sponsored agencies, organized crime, and other malicious entities desire access to the organization's IT information so that they can exploit it when planning potential attacks against national, state, and/or local infrastructures or commercial targets of interest.

Those attacks might and probably would include, among other things: network and system reconnaissance and the gathering of intelligence about

There still might be one critical type of “unnatural” disaster that emergency-response professionals have not considered thoroughly: a failure to protect the organization's own IT security strategy and its resilience to cyber attacks

the organization; the insertion of “Trojan Horse” programs that could be used to control the organization's systems (or to steal sensitive data); and/or the installation of destructive programs that might be used to deny the availability of these systems to their legal users during a period of critical need. In any time of crisis, this added destruction, misappropriation, or denial of service to the IT and/or telecommunications systems of the emergency-response community could

create grave problems for citizens dependent upon those services.

As with disaster-preparedness and business-continuity planning, the protection of IT security is an imperfect science – i.e., there is no way to create either a perfectly secure or “hardened” network infrastructure or a totally risk-free IT environment. However, there *are* sound and prudent approaches for discovering and managing IT risk that address these advanced and evolving threats, and that can help preparedness security professionals and emergency-response organizations build resilience into their IT systems and networks.

The Key Question In Risk Management: What Matters Most?

To close this cyber-security gap and to protect the organization's information assets, IT staff must not only understand the threat environment, but also plan and prepare to cope with potentially major cyber security problems. Best practices today in information security include the deployment of advanced network and system-level monitoring and risk-discovery systems both on organizational networks and on individual workstations and servers that can help alert the IT staff to the types of attacks mentioned earlier. Senior managers should think of these monitoring devices as alarm systems that would: (a) notify the organization of the presence of advanced threats; and (b) permit the IT staff to take action *before* a cyber problem affects a critical IT asset needed by the emergency responders.

Ideally, the monitoring and IT risk-discovery infrastructure would be able

to do any and all of the following: (1) Capture and analyze all inbound and outbound network data crossing the wires (to detect the numerous types of advanced threats that exist today); (2) Discover mission-critical data on all workstations, servers, and other “host” devices in the organization; (3) Evaluate the specific security condition of these IT assets; and (4) Alert, notify, and report the various software applications that can interface with the organization’s own communication systems (to ensure that IT staff not only can receive timely information but also take immediate action to deal with potential threats, vulnerabilities, and the IT risks that are of the greatest importance).

There are many types of cyber security-related issues that IT staff should monitor on a 24/7 basis. Cyber risks can come from inside or outside

of the network. When thinking about IT risks to the organization, it is useful to consider problems from a business point of view, and in that context see how increased monitoring and risk discovery may provide greater visibility into potential issues. Following are several IT “risk questions” that might well be asked to help determine the potential implications of a negative or at least suspicious finding:

- Why are data leaving the network to organizations or countries with which there are no legitimate business needs for communications?
- Why are large amounts of data being transferred in the middle of the night or during non-work hours?
- What are these new network services or applications running on the IT infrastructure?

- Which end-users on the network seem to be trying to evade organizational security policies by downloading inappropriate programs or files and/or by using rogue encryption?
- Who is carrying out research on firearms, other dangerous materials, or terrorist groups?
- Who seems to be storing or transmitting personal data on other employees (or on persons unknown) in violation of federal, state, or local regulatory requirements?
- What systems possess the largest concentration of sensitive or citizen data, but the weakest security controls?

For the preparedness or emergency-response professional, the availability, reliability, and resilience of the organization’s IT assets can literally mean the difference between life and death in times of crisis. In today’s world, unfortunately, organizations must plan for the worst-case scenario when considering how best to protect their information systems and IT assets. Implementing the recommendations above, particularly those related to the installation of a robust monitoring and IT risk-discovery infrastructure, can help any organization’s preparedness and emergency-response professionals not only protect their systems and networks from harm but also plan more effectively to avoid future cyber emergencies.

Amit Yoran, chairman and CEO of NetWitness, has been serving in those posts since November 2006. Prior to joining NetWitness, he was director of the US-CERT and National Cyber Security Division of the U.S. Department of Homeland Security, and before that was CEO and advisor to In-Q-Tel, the venture-capital arm of the U.S. Central Intelligence Agency. He also previously served as the vice president of Worldwide Managed Security Services at the Symantec Corporation.

HAS YOUR MEMBERSHIP EXPIRED?

YES!

I want to renew my membership!

Renewing your membership
is as easy as 1, 2, 3...

1. Visit www.DomesticPreparedness.com
2. Enter username/password, and make sure your profile is up to date
3. Enter this promo code: **RENEW**
All qualified professionals will receive a complimentary subscription.

Any questions? Problems logging in?
Contact our office (410) 518-6900; or email subscriber@domprep.com

The Beslan School Massacre

A Threat with No Easy Solutions

By Patrick D. Bird & Michael Allswede, Law Enforcement



"We offer you a sensible peace based on mutual benefit by the principle 'independence in exchange for security.'" Ruslan

Tagirovich Khuchbarov, "The Polkovnik"

Ruslan Tagirovich Khuchbarov, also known as *"The Polkovnik"* (Russian for "Colonel"), was the leader of the Chechen takeover – and the subsequent massacre of 396 students, parents, and teachers – of Beslan School Number 1 in the first week of September 2004. His "offer," quoted above, to local authorities demonstrates the common terrorism strategy of threatening the public and offering a false security in exchange for nonviolence. The standard official response, "not negotiating with terrorists," was used by Russian authorities and the conflict ended tragically. At 396 deaths, the Beslan School Massacre was the second most successful al Qaeda terrorist attack after the terrorist attacks against the United States on 11 September 2001.

The United States itself has spent little time or effort, unfortunately, in learning to cope with this type of event. Despite the Chechen attacks in 2002 against a Moscow theater (160 deaths), the Budyonovsk hospital attack in 1995 (105 deaths), the Mumbai financial district attacks in 2008 (179 killed), and Beslan, preparations for a suicidal attack-hostage crisis of similar magnitude have received little attention in the United States and almost no funding.

The attack on Beslan School Number 1 started not long after daybreak on 1 September 2004, the first day of school, when 25 or so members of the Chechen resistance, along with at

least two known al Qaeda members associated with the Finsbury Mosque in London, mixed into the crowd of students, parents, and teachers. Only the terrorists knew, of course, that, after repairs had been completed on the school during the previous summer, workers affiliated with the terrorists and/or sympathetic to their cause had hidden a number of weapons under floors and behind walls in the school. After mixing with the crowd going into the school, the Chechen attackers quickly retrieved the weapons and took 1,300 students, parents, and teachers hostage.

Ambiguous Reports And a Lethal Conflagration

All of the able-bodied men in the hostage group were taken to a courtyard and immediately executed; the remaining hostages were herded into the school's gymnasium, which was rigged with a series of incendiary bombs. A "dead man's switch" was used as a potential triggering device – i.e., a terrorist remained standing on a contact plate switch during the entire episode. If a rescue attempt was mounted, or if a sniper shot the terrorist, the contact would be broken when the "switch" terrorist serving as the contact either stepped off or fell off the plate, and the bombs would be detonated.

By the early dawn of 2 September Russian authorities had taken over from the local police, and the Russian "Alpha Team" (a special forces unit) was in command. Negotiations broke down after issuance of Khuchbarov's "independence for security" threat. On the third day, 3 September, the terrorists detonated the bombs – either after a rescue attempt or perhaps intentionally (the official reports are

somewhat ambiguous on this point). The resultant fire killed 344 hostages including 186 children, eight police officers and civilian bystanders, two emergency workers, and 11 members of the Alpha Team.

In addition, 437 hostages, including 221 children, were injured; many of them were suffering from burns, others from "crush injuries" (and subsequent limb amputations) caused by structural collapse, and some of them lost one or both eyes (hit by flying debris).

At least 19 attackers also were killed in what appears, in hindsight, to have been an intentional suicide attack. By the time the incendiary bombs were detonated, there were two ambulances on the scene as well as one fire truck (without water), but there had been little if any realistic preparedness efforts ordered or ongoing to deal with the flood of victims about to arrive at local hospitals.

Physical and Political Implications for U.S. Planners

The motivation for the Chechen attackers was similar in some respects to the anti-American motivations of al Qaeda and similar groups – namely, to avenge Russia's alleged oppression of Muslims. Beslan is a relatively small city in the predominantly Christian province of North Ossetia not too far north of the border between northwestern Iran and northeastern Turkey. Although the conflict in Chechnya was well known in Beslan, the attackers took advantage of the school's "open campus" atmosphere and relatively lax security. By hiding the weapons ahead of time, and attacking on the first day of classes, the Beslan terrorists were able to mix in with the parents, teachers, and other visitors and to avoid a possible interdiction of the attack later in the school year.

The ability of the United States to mount an effective response to a Beslan-like attack, almost anywhere in the country, is at best limited. U.S. schools are relatively open elements of society, including casual visitors, usually do not require ID cards, and, because they are intended for learning, designed to make it easy for a large number of children to be gathered together in group settings. Most American schools host a number of sporting events, concerts, plays, and assemblies – any of which could quickly be transformed into a potentially nightmarish security situation. Moreover, because so many school districts face limited funding, and are preoccupied with federal and state accountability mandates, school officials focus their attention, and financial resources, on meeting instructional objectives. School security, therefore, although important, is secondary to the school's principal mission.

Most U.S. school districts have developed and promulgated notional "Safety Response" plans, usually developed in cooperation with local law-enforcement and emergency-response agencies. Many of these same school districts also have created official safety-response teams, which meet from time to time both to review and update their response plans and, less often, to hone their response capabilities to cope with certain pre-planned exercise scenarios.

Few if any U.S. school districts, however, have any experience – even in the exercise scenarios – in coping with a full-blown terrorist attack similar to the Beslan attack. This rather glaring omission may be due, at least in part, to the psychological disposition of most school personnel. Educators and school administrators are (or at least are supposed to be) "nurturing" by nature and therefore not usually wired to think like attackers.

Theoretically, at least, this makes them less sensitive than they perhaps should be to exposing children to the possibility that a massive Beslan-type attack actually could occur in the United States itself. Putting it another way: Educators tend to protect students from thoughts that could frighten them, and that tendency is reinforced when statistics show that it is highly unlikely that U.S. school buildings could and/or would be attacked. Therefore, a built-in psychological vulnerability exists.

The attack started not long after daybreak when members of the Chechen resistance mixed into the crowd of students, parents, and teachers

The Columbine and Virginia Tech Exceptions

On the other hand, most U.S. school officials *are* particularly cautious in discussing the possibility that schools might be susceptible to attacks by an individual terrorist. Most if not all current school district plans are primarily focused, therefore, on "Columbine"-type attacks, or attacks by a single gunman, as at Virginia Tech. To prepare for a larger-scale terrorist attack, school officials would be well advised to consider the development of plans that include the use of a "scatter and rally" strategy (which would require students to run from the building if an attack has started and/or seems evident, and regroup later at one or more pre-designated rally points).

Although implementing such a strategy might save a number of lives, school districts are currently unable – for a number of reasons – to practice scatter-and-rally drills in a real-life setting. First, the risk of losing students and/or exposing them to the dangers of being unsupervised during such a drill is significant. Younger students could get confused and panic. Moreover, many parents – who are often critical of schools even for practicing simple lockdown procedures – would have an even more difficult time supporting the scatter-and-rally drills. Even if parents did support practicing such drills, they still would demand that the schools provide them with detailed information about the drills – but releasing that information would expose the specifics of the plan to potential attackers.

In addition – partly to save on construction costs, partly for other good and practical reasons – many if not all U.S. school buildings, particularly those in major metropolitan areas, are two or three stories high, not including the basement. Obviously, multi-story schools usually could not rely on a scatter-and-rally strategy if the school's first floor has already been secured by attackers.

There also are certain political and legal problems that must be resolved. To begin with, U.S. schools are almost by definition "weapons-free" zones. In addition, school personnel (except, in some school systems, security guards) cannot legally arm themselves – and even if they could they usually would lack the training needed to stop a terrorist attack without endangering the children (and, probably, the faculty). The quickest response, almost always, would have to come from trained professionals – who, of course, would not be able to respond until *after* an attack group had

Most Biohazard Detection Systems Come with a 20% Error Rate



Shouldn't You Be More than 80% Prepared for an Attack?

Instruments using antibody-based detection are less reliable because of their high false negative rate. Their results need to be verified at a separate lab using PCR. Idaho Technology's portable biohazard detection system, the RAZOR® EX utilizes the same PCR technology that health labs use without a need for in-depth knowledge of the science behind it. The RAZOR EX was made for HazMat and first responder teams that require more from a detection system.

The RAZOR EX is a complete product solution that is easy to setup, run, and read. Capable of testing ten bioterrorism agents in one run, the RAZOR EX provides more accurate results than other products in less than 30 minutes.

Visit our web site or call today and let us help you get the most trusted and accurate field portable detection system into the hands of your team.

Turn Your False Negatives Into Cash



Idaho Technology has many ways to help you get the best products for your team. For example, take advantage of our trade-in program by giving us your inferior antibody based detection system for cash towards the purchase of our more reliable PCR based detection system.



The RAZOR® EX with rugged carrying case



Innovative solutions for pathogen identification and DNA research

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

already taken over the school. This last problem would be especially true in more rural areas.

Applying Lessons Learned From the Beslan Attacks

The best predictor of future behavior is past performance. As the incidents cited earlier prove, combining a suicidal attack with the taking of a large number of hostages multiplies the terrorists' motives, and results, by ensuring additional media coverage of what could be an extended siege. The terrorist demands also would receive considerably more publicity.

The United States would be particularly vulnerable to the same terrorist strategy because its primary and secondary schools, colleges and universities, commercial centers, and leisure-time venues are quite literally open targets. With all due consideration given to the potential detonation of a terrorist nuclear bomb and other homeland-security planning scenarios designed to protect high-visibility and/or critical-infrastructure targets, American counter-terrorism planners should also evaluate and plan for the simpler but easier and perhaps more effective attacks against less obvious targets.

The simplistic response to this dilemma would be to create a perimeter-control or "Fortress America" strategy, similar perhaps to what Israel has had to do. The problem with this strategy is that it never could be completely effective, even in Israel's relatively homogeneous society. The Israeli people may not like it, but they accept, as a fact of modern life, the presence of armed teams of security personnel on school property and at school events. The application of the same type of security concepts to the American melting pot would be less easily accepted and therefore would also be less effective.

Response planning or "target-hardening" might be a more useful strategy to consider. The development of a scatter-and-rally strategy – when combined with total-lockdown strategies for schools, universities, and other educational facilities – might be particularly useful. Terrorist hostage-takers rely on a combination of: (a) total surprise; and (b) their own ability to quickly collect and control hostages in a confined area. The development of a rapid, random, and frequently *practiced* scatter strategy – with carefully defined

The quickest response, almost always, would have to come from trained professionals – who would not be able to respond until after an attack group had already taken over the school

and pre-designated points for the recollection of students – could be a useful counter-strategy against a Beslan-type attack. Here it should be noted that at least 50 potential hostages escaped from School Number 1 by running away immediately, as individuals or in small groups, in the early moments of the 2004 attack.

The community under attack obviously must be well organized for the large-scale response needed. An attack on the Beslan scale, or the several simultaneous attacks last year on several pre-designated targets in Mumbai, would be a major challenge for even the most experienced

ICS (Incident Command System) leader. The lack of fire-suppression capabilities and the failure of Beslan officials to prepare their own hospital resources faster and more effectively probably added significantly to the death count. Many victims who had not been injured by the initial blast and attack were injured in the subsequent fire and/or the rescue melee that ended the incident. Other victims, suffering from survivable injuries, died because of the lack of a well organized and adequately prepared medical response.

To quickly summarize: The global patterns of suicidal, hostage-taking attacks have shown a trend of increasing success for the terrorists that has not been given adequate attention by American planners. Such attacks are relatively low in cost for the terrorists, extremely dramatic in their effect, and almost always successful in focusing world attention on the demands of the terrorist group involved. Until successful detection and counter-strategies can be developed, terrorist groups will have little incentive to change. The cost of *not* preparing for suicidal hostage-taking attacks will therefore serve as an open invitation to terrorists to launch even more such attacks in the future.

Dr. Patrick Bird (pictured) is a superintendent of schools in Michigan and holds a PhD in educational administration from Iowa State University. He also is an adjunct professor at Saginaw Valley State University, where he teaches graduate courses in leadership theory and personnel management. He also serves on a local emergency planning and response team and has managed a number of school crises in urban, suburban, and rural schools in Texas, Iowa, and Michigan.

Dr. 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.

Isolation, Quarantine, & the Compression of Time

By Joseph Cahill, EMS



Isolation and quarantine: Although the two words seem interchangeable to many people, in public-health circles they are not; the principal difference between them is who they affect, and why.

Isolation refers to secluding a sick patient to keep him or her from spreading the disease or to keep a patient with a weakened immune system from becoming further infected. Patients can be isolated in special rooms either in a hospital or, if their condition allows, in their own homes.

Quarantine, on the other hand, refers to secluding healthy or “well”

people who have come into contact with a sick person. The goal of both isolation and quarantine is to keep all potentially infected, and therefore infectious, people away from those who are not infected. If action is taken fast enough, the isolation and/or quarantine strategies can help to contain the spread of a disease.

The Exponential Growth Of International Travel

One of the major differences between the world of the early 20th century – when the 1918-19 global influenza pandemic claimed the lives of an estimated 50 million people throughout the world – and today’s world has been the development and growth of rapid international

travel. American troops waiting for deployment to Europe in 1918 were sequestered for several weeks in U.S. military bases on the east coast of the United States, then transported to Europe on relatively slow-moving troop ships. Even for those embarked on the speedy new ocean liner *Queen Elizabeth*, the trip took at least six days. Today the same trip takes only six hours – by air.

During the same several decades when travel time was being compressed from a few days to only a few hours, the number of international travelers was increasing exponentially. Except for the troops, only the rich and super-rich, plus a few scholars and

FIRST RESPONDERS NEED TO BE PREPARED FOR ANYTHING...

SO DO OUR SUITS

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

USA Tel: +1 866 803 5956
Email: frontline@remploy.com

UK Tel: +44 (0)845 241 2990
Email: frontline@remploy.co.uk

www.rememployfrontline.com

Remploy Frontline

SURVIVAL EVOLUTION

students (many of whom “worked their way” overseas), could afford to and were able to travel abroad in the first two decades of the 20th century.

Today, hundreds of thousands of people, from almost every country on the planet, cross the oceans every day in huge passenger aircraft that soar over the world ocean at speeds previously undreamed of. The Delta flight from Atlanta, Georgia, to Mumbai, India – to cite but one example – takes only 17 hours. Theoretically, in fact, it is now possible for any person anywhere in the world to travel to any other place in the world in less than 24 hours.

Diseases Also Travel Faster

The lethal corollary of these advances is that when people can travel that fast, the diseases they carry with them are traveling at the same speed. Add to that the fact that, according to the World Health Organization (WHO), a person who has been infected can infect others even before he or she displays visible symptoms. In 1918, an infected person would in all probability have exhibited such symptoms long before arriving at his or her destination.

Using modern transportation, though, a traveler can be in Mexico City today, in Germany for a meeting the following day, and off to China the day after that. The net effect is that an infected person may complete such a three- or four-day itinerary well before starting to show any symptoms.

In dealing with the current Swine Flu/H1N1 influenza outbreak both WHO and the U.S. Centers for Disease Control and Prevention (CDC) – working in close cooperation with other national and international public health agencies – have relied

primarily on a mixture of travel warnings and restrictions to at least partially cope with the rapidly rising number of confirmed cases reported in one country after another in all corners of the world.

The Belated “Race Against Time”

In many cases the principal response from these agencies was

One of the major differences between the world of the early 20th century and today’s world has been the development and growth of rapid international travel

the issuance of recommendations to the general public to avoid unnecessary travel to areas known to have already been affected. Of course, by the time those recommendations were issued the disease was already past the point of being contained by travel restrictions.

On an international scale, restrictions on travel to an affected country can be viewed as either isolation or quarantine, depending on the direction and duration of the restriction. The global nature of business, educational, and recreational travel makes restrictions on travel extremely difficult both to put in place and to enforce. WHO issued the following statement in

regards to the present H1N1 2009 outbreak, in fact: “Limiting travel and imposing travel restrictions would have very little effect on stopping the virus from spreading, but would be highly disruptive to the global community.”

Another major difference between today’s travel conditions and those prevalent in the early 1900s is the current availability of instantaneous international communications. Epidemiologists can now use the internet to share information in the blink of an eye that a century ago would have been globally “disseminated” no faster than the speed of ships. The rapid growth in communications capabilities allows quicker warnings, therefore – and, possibly, a more rapid understanding of an outbreak, but not its actual prevention.

For that reason alone, and even though “closing borders” might seem to many to be an obvious (and politically tempting) response to the outbreak of an infectious and potentially deadly disease – that option is not backed either by science or by the everyday facts of daily life in the 21st century.

Joseph Cahill, a medicolegal investigator for the Massachusetts Office of the Chief Medical Examiner; previously served as exercise and training coordinator for the Massachusetts Department of Public Health, and prior to that was an emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as the citywide advanced life support (ALS) coordinator for the FDNY - Bureau of EMS, and prior to that was the department’s Division 6 ALS coordinator, covering the South Bronx and Harlem. Much in demand as a speaker - he has addressed venues as diverse as the national EMS Today conferences and local volunteer EMS agencies - Cahill also served on the faculty of the Westchester County Community College’s Paramedic Program and has been a frequent guest lecturer for the U.S. Secret Service, the FDNY EMS Academy, and Montefiore Hospital.

Field Testing or LRN Laboratories – Why Not Both?

By Rob Schnepf, Fire/HazMat



A true dilemma occurs when a choice must be made between two approximately equal and perhaps unappealing alternatives. The phrase

“being between a rock and hard place” is a well known example of having two choices, neither of them very desirable.

Presumptive screening in the field vs. more definitive testing in a laboratory represents the “rock” and the “hard place” in many discussions about the identification of biological agents. Proponents of field-level detectors of biological agents – for example, District Chief Armando Bevelacqua of the City of Orlando Fire Department – are firm believers in the value of field screening. “There is an expectation that public-safety [agencies], especially the fire department,” Bevelacqua points out, “... [are] capable of handling suspicious powder calls. We are looked at by the general public as all-around problem solvers.”

That public expectation, it seems obvious, includes a belief that the problem solvers mentioned possess both: (a) the training and expertise needed to determine if a threat is credible; and (b) the ability to use reliable field-detection instrumentation to make tactical-level decisions – very quickly. The tactical-level decisions just mentioned encompass such matters as returning a facility to normal operations after a hoax, offering peace of mind to persons who believe they have been “exposed” to a suspicious powder, and/or returning students to their classrooms after a white-powder scare.

“Reliable field testing,” Bevelacqua emphasizes, “gives you the ability to make informed decisions about the credibility of a potential situation

or substance.” But it is the need for reliable results that most concerns those who believe that field testing produces questionable results.

A Major Decline in False Positives

In any discussion about the reliability of field tests, the first questions usually raised are about the possibility of false positive results. False positives occur when a device signals that a particular agent is present when it is not, thereby creating a situation that shakes the confidence of the on-scene user and leads to numerous problems for emergency managers and other officials who must make decisions based on the results of field tests. Here it should be noted that, as recently as seven or eight years ago, field tests were in fact highly prone to false positive readings. Since then, however, the rate of false positives has dropped dramatically, in large part because of the maturing of the overall market. As a result, in the last few years the entire field-testing marketplace has improved significantly in terms of reliable performance.

It is still true, of course, that some manufacturers continue to make unsubstantiated claims about the performance levels of their products, but not all technologies are suspect. There are, in fact, some very reliable and validated instruments available to the first-responder market. When those instruments are used by trained responders, the results obtained in the field will also be reliable.

Among the most rapid and reliable field-testing devices are those that use PCR (polymerase chain reaction) technology to make their assessments. Those assessments are extremely specific because the PCR technology identifies the DNA of the test sample – an obvious benefit to first responders.

Once limited to use only in the laboratory, more user-friendly PCR devices are now making their way into the first-responder market.

These devices are similar in concept to laboratory testing methods – with the added advantages that they are portable, capable of withstanding the rigors of field use, and relatively easy to operate.

Experts in the hazardous materials response field agree that the laboratory testing of biological agents is still the “gold standard” in the detection field, but the highly respected Laboratory Response Network (LRN – established in 1999 by the U.S. Centers for Disease Control and Prevention (CDC) – is not a 24/7 operation. Even in most major metropolitan areas, the LRN – which links federal, state, and local labs together in a truly national network – is not as quickly available as most local fire and police departments, and there are times when that unavailability becomes unacceptable.

The Gold Standard Vs. Intangible Skills

One can easily imagine a situation in which a suspicious powder is found inside a busy shopping mall, in a large city, at the height of the Christmas shopping season. The entire mall might have to be evacuated, and thousands of dollars an hour in probable sales would be lost during the period when the mall is closed. Without a trained and properly equipped first-responder corps that can be on the scene on very short notice, the facility is at the mercy of the LRN, and could be closed for several hours, or even days, because there would be no reliable way to make a relatively quick decision about the nature of the suspicious substance. In that scenario, one of the major benefits provided by field screening

would be that immediate information *would* be available about the substance in question. That information may not be quite as ironclad as the information obtained from culturing the sample in a lab, and/or using other high-end testing methodologies, but there is growing empirical evidence suggesting that, when trained responders use highly reliable instruments to make informed decisions, the usual result is a high percentage of accuracy. Keeping in mind the fact that there is a significant difference between analyzing a *substance* and analyzing a *threat*, it seems that the principal difference, therefore, between relying on the LRN and relying on the first-responder community is the intangible skill of assessing the incident (threat) as a whole, not just the substance itself.

Local responders are in that respect somewhat like “a triage center for the laboratories,” Bevelacqua says. “If the threat looks ... credible, and the sample tests positive in the field – or we’re not sure about the results – the labs are going to get the sample anyway. That’s the way the process works. All we do is weed out the [potential threats] ... that are clear-cut hoaxes.”

Viewed in that context, it seems that there is perhaps no real dilemma when deciding about the merits of testing a substance in the field instead of in an LRN laboratory – each method of testing serves a separate and distinct purpose. In other words, rather than seeing field testing for biological agents as a competitor to the LRN, or vice versa, the logical, and more practical, view should be of a cooperative situation, with each alternative having its own appeal as well as its own place in the overall identification process.

Rob Schnepf is the Chief of EMS and Special Operations for the Alameda County (CA) Fire Department. He is the author of a textbook entitled Hazardous Materials: Awareness and Operations, by Jones and Bartlett Publishing. Rob is a member of the NFPA Technical Committee on Hazardous Materials Response Personnel.

License Plate Readers: Automated Situational Awareness

By Rodrigo (Roddy) Moscoso, Law Enforcement



The use of License Plate Reader (LPR) technology by law-enforcement agencies has increased heavily in recent years, thanks primarily to significant enhancements in the technology’s underlying hardware and software. Weatherized digital cameras can now quickly capture high-resolution images of passing vehicles, and the mobile computers to which they are connected have the processing power needed to analyze a fast-moving stream of license-plate images. This capability enables law-enforcement officers to quickly canvass a parking lot by simply driving through all of the lanes in the lot while the cameras and computer in the police vehicle automatically check for stolen cars, stolen license plates, and/or wanted persons registered to those vehicles.

Previously, officers would be forced to enter each license plate number individually into their mobile computer query systems. Although touch screens and voice-recognition technology can simplify human input to some degree, the capability of LPRs to quickly scan and check a large number of license plates in a very short time makes any form of human input pale by comparison. The operational process used is also much safer than attempting to type license-plate numbers into a mobile computer while driving.

The next technological leap for LPR technology lies in bringing its impressive optical and processing capabilities into the realm of real-time “connected law enforcement” information sharing. Today, most LPR systems compare the results

of their scans to a local database, stored on their mobile computers, of vehicles on a current “wanted” list. The database is typically downloaded to the mobile computer by way of “thumb” drive, WiFi, or office LAN and is usually as much as a day old (and sometimes older). If a vehicle is reported stolen after the database has been downloaded, the LPR would ignore license plates not in the locally stored database because they would not be listed there.

However, current LPR software does provide an interface for officers to manually add a license plate to the local database – if alerted by radio dispatch, for example, of a recently stolen vehicle. This process, though, is not yet automated and therefore depends on the availability of an officer both to hear the alert, and then to take the time to enter the newly received information into the mobile computer.

Instant Updates And Immediate Implications

Today, fortunately, the existing communications capabilities already integrated into most mobile computers provide a way, using LPR technology, to enable the real-time transfer of extremely recent law-enforcement data. In fact, some LPR systems, if properly networked, can use wireless broadband networks – e.g., Verizon and AT&T 3G – to transmit updates to field cameras.

The implications for improving law-enforcement responses are significant. For example, vehicles identified as stolen (or registered to newly wanted persons) could be automatically

“pushed” to LPRs in police vehicles and/or mounted at fixed locations. In either case, the LPR systems could immediately return a “hit” if the vehicle is scanned at any time from that point forward.

Another significant added value provided by LPR technology is that the newer systems also can store the scans made during a given shift or time period. This means that a large amount of potentially critical information, including the time and GPS (global positioning system) location for each license plate recently stored, is recorded and therefore can be quickly cross-referenced with updated information. For example, if a subject vehicle had been scanned only minutes prior to the receipt of an electronic BOLO (“Be on the Lookout”) message, the system could instantly inform an officer in the field not only that the vehicle had been recently scanned but also where and when the scan took place. The combining of a number of recent scans from several LPR systems could therefore quickly paint a picture of a vehicle’s immediately previous locations and possibly identify a direction of travel or provide other helpful information.

The same technology may prove extremely beneficial to lookout alerts encompassing a relatively large geographical area. For example, in October 2002 the greater Washington, D.C., area was terrorized by the infamous sniper attacks, which stretched from Washington, D.C., and its Maryland suburbs 90 miles south into Virginia. Making the situation more complicated was the fact that early eyewitness reports wrongly identified the vehicle used in the sniper shootings as a “white box van,” a description that led law-enforcement personnel to focus their attention on the wrong type of vehicle.

Erroneous Information Results in a Fruitless Search

A system of “connected” mobile and fixed LPRs might have helped in that investigation by focusing on the identification of vehicles that had been scanned near the times and locations of two or more of the attacks. The systems would not be

Existing communications capabilities already integrated into most mobile computers provide a way, using LPR technology, to enable the real-time transfer of extremely recent law-enforcement data

specifically looking for a white box van. Instead, they would be looking for license plates of vehicles that were known to have been in the proximity of at least two of the several crime scenes at about the same time of two or more of the sniper attacks.

Of course, to create a regional system of connected LPRs would require the standardization of several LPR technologies and the exchange of data across two or more political jurisdictions (usually, though, within the same geographical area). In addition, a regional system of electronic BOLOs would be needed to provide real-time dissemination of information across several LPR networks.

Fortunately, new regional data-sharing systems are already operational in many jurisdictions and could be used for just that purpose. By marrying the technologies and capabilities now in place, newly available features could be further exploited – by the issuance of alerts triggered by what is known as “Geo-Fencing.” One example: If the vehicle owned by a registered sex offender is scanned by an LPR system while that vehicle is physically located in a school zone, the system can alert an officer in the same general vicinity (but no alert would occur if the scan occurred outside of the zone). Finally, the wealth of data being captured by LPRs could be easily exported into a standard XML (extensible markup language) format, thereby making integration with new and robust analytic tools possible across a wide regional area. Such an upgrade could quickly add a new and powerful information layer – and operational capability – to emergency managers and homeland-security officials at all levels of government.

In short, all of the components are already in place to better leverage LPR technology and capabilities to improve law-enforcement operations. What is needed now are strategic coordination, multiagency cooperation, and the political will necessary to make better use of technologies already developed and in the field.

Rodrigo (Roddy) Moscoso currently serves as Communications Manager for the Capital Wireless Information Net (CapWIN) Program at the University of Maryland. Formerly with IBM Business Consulting Services, he has over 15 years of experience supporting large-scale IT implementation projects, and extensive experience in several related fields such as change management, business process reengineering, human resources, and communications.

A Change in Fashions for the Well-Suited Responder

By Glen Rudner, Fire/HazMat



Today's first-responder community is continually searching for the most effective technology to provide protection during a hazardous materials or WMD (weapons of mass destruction) incident. However, because most incidents to which first responders are dispatched do in fact involve hazardous materials, it is imperative that the responders are wearing or have with them the personal protective equipment (PPE) appropriate both to the hazard and to the response objectives. U.S. and allied manufacturers are for that reason trying to meet the triple challenge of not only keeping up with the technology available and the PPE standards established – by both the U.S. government and several non-government organizations such as ANSI (the American National Standards Institute) and NFPA (the National Firefighters Protective Association) – but also adhering to the cost limitations that the responders are asking for.

Since the early 1980s, numerous standards and regulations for chemical protective ensembles have been developed to assist both the responders and those who work with hazmat materials on a daily basis. The push for better – i.e., safer, more comfortable, and reasonably priced – PPE gear has been driven, at least in part, by incidents such as the tank car leak of anhydrous dimethylamine in Benicia, California, that helped persuade the standards organizations and regulatory agencies to establish more stringent minimum-performance standards for chemical protective clothing ensembles.

In recent years, several new standards and regulations, more comprehensive

than their predecessors, have been published and kept updated to meet the needs of the responder community. Among the more important of them are NFPA 1991 Standard on Vapor-Protective Ensembles for Hazardous Materials Emergencies, the NFPA 1992 Standard on Liquid Splash-Protective Ensembles and

Responders can choose a suitable respirator only after they have evaluated all relevant factors involved, specifically including the limitations of each type of equipment available

Clothing for Hazardous Materials Emergencies, and the NFPA 1994 Standard on Protective Ensembles for First Responders to CBRN [chemical, biological, radiological, nuclear] Terrorism Incidents. These and several others have become extremely useful tools for responders choosing the PPE needed for their personal safety.

Leveling the New Ensemble Playing Field

One of the more important definitions found in the NFPA standards, which are written specifically to help responders choose the appropriate protective equipment, is the term “ensemble.” The responder has to look at the individual chemical protective equipment items that he (or she)

chooses as separate components of the ensemble as a whole. The suit, boots, gloves, respiratory equipment, and various accessories make up the ensemble, and each of those individual equipment items must be thoroughly researched prior to being purchased and used on a response.

Unfortunately, there is what might be called a “language problem” that has caused a lack of understanding, and sometimes outright confusion, within the response community when it comes to choosing the whole ensemble. The official standards and other documentation used to describe PPE items usually refer to the equipment as ensembles, but many members of the response community use shorter and more easily remembered names for the same equipment – “Level A,” “Level B,” or “Level C” suits, for example, rather than the “official” ensemble names. The official names come from EPA/OSHA (Environmental Protection Agency/Occupational Safety and Health Administration) guidelines and are both longer and more difficult to remember.

The separate equipment items making up the ensemble need to be researched individually when a response mission is tasked. However, the same changes in technology that have made PPE gear more effective have at the same time made the choice of ensembles a greater challenge than in the past. For example, the newer versions of NFPA 1991 require that all materials

**View ATI
(Air Techniques International)
Product Profile**

OUR MISSION YOUR SAFETY

MSA
The Safety Company



TRIPLE RESPONSE

With MSA's NEW
FireHawk® M7 Responder
Air Masks

- 1 Use FireHawk M7 CBRN SCBA for firefighting and rescue
 - 2 Switch to FireHawk CBRN Gas Mask (*air-purifying respirator*) for scene management, after low hazard level is assessed
 - 3 Convert to FireHawk CBRN PAPR (*powered air-purifying respirator*) for long-term comfort and use
- Each mode meets/exceeds the latest requirements of NFPA & NIOSH standards.

RESPOND NOW!

Call your MSA fire service distributor or go to MSAFIRE.com.



| SCBA | APR/PAPR | FIRE HELMETS | GAS DETECTION | THERMAL IMAGING CAMERAS |

1.877.MSA.1001 | www.msapoliceline.com/domprep.html

View
ILC Dover
Technology Briefing

used in construction of the suit – base material, seams, and closures – must demonstrate resistance against various chemicals (the boots and gloves must meet that same requirement). Some manufacturers were unhappy about the more stringent procedures required under the new testing standards, but the end result was that this added challenge caused the manufacturers to reevaluate their current products and develop new materials more suitable to the responder community's needs.

Following are some of the factors involved in selection of the specific equipment items indicated:

Gloves – Most responders today use two or more layers of gloves to protect themselves against the hazards of an incident. From the innermost gloves – made of Nitrile materials to provide the last layer of protection against chemical/biological exposure – to the outermost glove, which is made from leather to protect the wearer's hands and fingers from mechanical damage, hand protection is always, and necessarily, a high-priority equipment item because well designed gloves facilitate the manipulative skills needed to mitigate hazmat effects and/or sample potentially hazardous materials during a hazmat response.

The number of *pairs* of gloves that should be worn by the individual responder is based on the need for protection against several hazards. Among the questions that should be asked before selecting gloves are the following: What are the general hazards of the product? Are there

mechanical hazards likely? What are the dexterity needs?

Boots – Responders who are working at hazardous materials/WMD incidents, wear leather fire/work boots, rubber boots, etc., that must meet the specifications of ANSI Z41 1991. The *materials* used to make the boots are not usually subject to any specific standard; however, the *construction* of the boot is. Depending on the type of hazard

The changes in technology that have made PPE gear more effective have at the same time made the choice of ensembles a greater challenge than in the past

and the specific product, for example, the boot should protect the wearer against both liquids and solids. That requirement usually translates into a boot made of neoprene, polyvinyl chloride (PVC), butyl rubber, or any of several other materials that are available today.

Most if not all of the boots now used by responders come in different configurations to suit the needs of the individual user. They are available either as a shoe boot or as a "pullover" boot. Pullovers are less expensive and usually considered to be disposable. When wearing chemical-resistant shoe-boots, the responder should first slip his or her feet into the boots to ensure a comfortable fit; a protective rain flap will then go outside and over the boots to prevent liquids from entering.

Respiratory Equipment – Choosing respiratory protection is not a complicated matter. Once a specific hazard has been determined and the level of protection (OSHA/EPA or NFPA) needed has been decided, the type of respiratory protection required is almost automatic. However, responders can choose a suitable respirator only after they have evaluated all of several relevant factors involved, specifically including the *limitations* of each type of respiratory protection equipment available. The first priority should be identification and evaluation of the respiratory hazard. After those tasks have been done, there are several important questions that should be asked, including the following:

- Is the specific equipment item to be used in firefighting and/or hazardous material/WMD emergencies?
- Has the atmosphere been monitored for oxygen, flammability, and contaminant levels? Here there are several supplementary questions required: (a) Is the atmosphere oxygen-deficient (less than 19.5 percent oxygen in air)? (b) Is the airborne contaminant a gas, a vapor, or a particulate (mist, dust, or fume)? (c) Are the airborne levels below or above the exposure limit – and/or are they above levels that could be immediately dangerous to life or health?
- What are the operational conditions – e.g., cold/hot temperatures, confined space, etc. – most likely to be encountered?
- What is the specific mission of the individual responder (e.g., rescue, recon, retrieval, etc.)?
- How long will the mission last – i.e., how long will the responder have to wear the respiratory equipment?

Although not a complicated process, the selection of respiratory equipment does require the preceding and possibly a few other questions to be answered. In today's environment, fortunately, the technology already developed and available for purchase alleviates some of the selection problems. A good example is that the face-piece used with today's self-contained breathing apparatus (SCBA) can be adapted for use as an air-purifying respirator or a powered air-purifying respirator.

Chemical Protective Clothing –

The purpose of chemical protective clothing is to protect the wearer against hazardous liquids, gases, or vapors. Most of the clothing now available comes in a large array of styles and materials. The choice of what to wear is or should be based on the information available to the responder upon his/her arrival at an incident. Depending on the specific hazard(s) encountered, the responder can choose minimal protection or any of several intermediate levels of clothing up to the highest level. Many of the materials now available allow the responder to make choices based on the suitability of the specific material to the specific hazard encountered. The protective clothing may be made of Tyvek or Coated Tyvek, for example, both of which are durable, or of Nomex, which also is fairly durable and provides better flammability protection. All of these materials are usually categorized as "limited-use" – disposable, in other words.

As the hazards to the body progress in size and/or complexity, so does the level of protection needed. The materials that are used – e.g., polyvinyl chloride – become more complex, and therefore may be more suitable for liquids, which are stronger corrosive materials.

This will provide for minimal contact with the materials. From a cost perspective, some may be inexpensive enough to be disposable.

As a hazardous material presents an even a higher level of toxicity, additional protection is necessary. Materials such as the neoprene and butyl rubber mentioned earlier are good barriers against toxic hazards. Both of these materials are designed to provide a higher level of protection because of their ability to stop toxic hazards from entering the material worn by the responder. Once an



incident reaches the highest level of toxic vapor/gases, though, the requirement for the most complete protection available becomes mandatory. Today, the highest level of protection is the fully encapsulating suit. These suits are designed to totally block any permeation, penetration, or degradation by the chemical hazards to which the suit (and the wearer, of course) is exposed. All closures, including zippers and seams, also are specially designed and fitted to resist the chemical vapors/gases that the wearer will encounter.

Circulation, Perspiration, And the End of a Tradition

There are many problems encountered by the wearer of protective clothing, the primary one being that his or her body is shielded not only from dangerous chemicals but also from the normal circulation of air. Moreover, his/her perspiration does not evaporate, thus eliminating the body's own principal mechanism for cooling. The addition to the

protective suit of one of the several new technology-driven cooling systems is therefore necessary to help the wearer's own hypothalamus (the body's thermostat) reduce his/her body temperature immediately in a heat-stress situation. Heat-related problems are very common when the ambient temperature climbs above 75 degrees F.

To briefly summarize: The selection of appropriate personal protective equipment is based on several key factors, including the mission of the response team and the hazards anticipated or immediately recognized. Protective clothing protects the wearer primarily because of the materials from which the clothing is made. Today's hazardous materials/WMD responder has many choices in personal protective equipment available. Those choices should be made primarily on the basis of providing greater safety to the responder.

The practice known as "risk-based response" has evolved to the point that the best protection available can and should be made on the basis of hazard assessments completed by responders on the scene in the early stages of an incident. The old, heroic, and time-honored procedure of first responders arriving on the scene of a dangerous incident and immediately rushing into action is a relic of the past and has no place in the 21st-century world of terrorist attacks, mass-casualty incidents, and warehouses stacked from floor to ceiling with a host of lethal chemicals and other toxic materials.

Glen D. Rudner is the Hazardous Materials Response Officer for the Virginia Department of Emergency Management; he has been assigned to the Northern Virginia Region for the last nine years. During the past 25 years he has been closely involved in the development, management, and delivery of numerous local, state, federal, and international programs in his areas of expertise for several organizations and public agencies.

Mass Prophylaxis: The Brass Ring of Public Health Preparedness

By Bruce Clements, Public Health



There is no other public health preparedness objective that has received the effort, emphasis, or funding of mass prophylaxis. When one considers the impact it may have, it is easy to see why. Among the fifteen DHS (Department of Homeland Security) planning scenarios – spelled out more than two years ago in accordance with Homeland Security Presidential Directive 8 – are several related to biological outbreaks or attacks that offer the greatest window of opportunity for lifesaving interventions. The possibility of biological attacks using *Yersinia Pestis* or *Bacillus anthracis* – the causative agents of plague and anthrax, respectively, both of which have a delayed impact on health – is of particular significance. If the appropriate antimicrobial medication is received early enough, those exposed can avoid illness. If there are delays, deaths occur.

The Cities Readiness Initiative is the primary U.S. effort to enhance the speed and effectiveness of mass prophylaxis. The goal of the program is to get antibiotics into the hands of an entire metropolitan area population within 48 hours. This initiative has focused primarily on the use of “Points of Dispensing,” or PODs. Using this approach, stockpiles of antibiotics called “push packages” maintained in the Strategic National Stockpile (SNS) are sent to PODs where local public health authorities and volunteers can dispense the medications to individuals at risk.

Through regular exercises at major cities across the nation, it has been clearly demonstrated that reliance on PODs alone is not sufficient. After a local surveillance system, such as environmental monitoring

(BioWatch), or the epidemiological monitoring of human illness, detects a threat, the stockpiled drugs are deployed to the area of concern. The push packages are then broken down and sent to the PODs. However, the PODs still must be set up and the public notified where to go for prophylaxis. Finally, the dispensing begins. Each of these steps takes time. However, even though state and local public health professionals have made vast improvements in streamlining the process in recent years, it is still not possible to successfully treat most people living within a major metropolitan area in 48 hours or less.

The USPS Approach – Escorted by PPE Problems

Recognizing that the POD approach alone is not the answer, senior officials have ordered that other distribution approaches be considered. Perhaps the most promising of those alternate approaches has been the use of the U.S. Postal Service (USPS). There is no other system in place that touches every home in every U.S. community almost every day. Basically, the USPS approach would place prophylactic medications, and accompanying instructions, in the mailboxes of every home within an affected region in order to buy time for a more thorough follow-up using the PODs.

However, USPS officials have now defined what they need to carry out this task. Prominent among those needs are armed escorts as well as personal protective equipment (PPE) for USPS employees themselves. While these seem like reasonable requests, the “needs list” triggers all sorts of unwieldy requirements. Providing PPE for all (or almost all) USPS employees would mean, for instance, that they would have

to be fit-tested and maintained on a Respiratory Protection Program. In addition, it seems likely that, if USPS workers themselves are wearing PPE gear, their armed escorts would want similar protection – which probably would translate into placing all local law-enforcement officers on a Respiratory Protection Program. (Here it should be noted that some communities have already determined that they do not have enough law-enforcement personnel available to assign one to each USPS carrier.)

Another insightful approach being taken by some metropolitan areas is to recruit large employers to set up PODs for their own employees. This would be an immense help. Much of the mass-prophylaxis planning to date has *not* included employer stakeholders. It stands to reason that employers have a vested interest in assuring the health and safety of their employees and their families during a public health emergency. Their involvement is long overdue.

The problem is, though, that this approach has not been well planned and/or exercised in most areas of the country. Moreover, no one knows exactly how willing the major employers in some regions may be to assume this responsibility. Of course, in the aftermath of a disastrous incident or event, many undoubtedly would step forward and be willing to assist, not only as good citizens but also for the sake of business continuity. Nonetheless, the willingness of such employers to preplan and engage in the process *prior* to an event is still limited in most regions.

Is Pre-Placement The Final Answer?

Which leaves what may well be the final option: stockpile pre-placement

14th International Conference

Biodetection Technologies 2009

Technological Responses to
Biological Threats

June 25-26, 2009



KNOWLEDGE FOUNDATION

TECHNOLOGY COMMERCIALIZATION ALLIANCE

participating organizations:



www.knowledgefoundation.com

– which has in fact already been successfully carried out, albeit on a small scale, by some first-responder organizations. There are numerous fire, police, EMS, healthcare, and public health agencies and organizations across the nation that already have established local stockpiles for critical staff and their families. However, although the pre-placement concept seems sound enough in itself, there has been very little data developed to support the policy decisions needed to allow the pre-positioning of medications for homeland-security purposes.

Probably the last bastion for the pre-placement of prophylactic medications would be the homes of individual citizens. This option would in all likelihood be the most controversial and challenging approach to mass prophylaxis. There are, in fact, many healthcare professionals who feel strongly that the pre-placement of antimicrobial drugs in homes would be a potentially catastrophic mistake. The medications might be used inappropriately, and/or be improperly stored, and therefore might pose more risks than benefits to the households maintaining them.

In light of recent trends toward antimicrobial-resistant organisms, this is a noteworthy concern. If the diseases the nation has managed for decades, mostly by using antimicrobial drugs, continue to build resistance to those therapies, it may well be that previously treatable illnesses become untreatable.

The improper use of home “Medkits” could contribute to the problem. The dilemma here is that there are no data either to support, or to refute, the assumption that these drugs, if kept in a home for homeland-security purposes, would contribute

to and/or exacerbate the mounting public health challenge posed by antimicrobial resistance. Moreover, it has never been done before – not, at least, in the United States, which has never packaged medications for household preparedness or even carried out a major test program to determine how responsible the general public may be in handling them.

However, an initial study on the potential household placement of antimicrobials was carried out in 2006 and 2007 in an area in and around St. Louis, Missouri. A convenience sample of homes was selected for the study, and a prototype Medkit was created for the test. The kit contained a five-day supply of either doxycycline or ciprofloxacin, sealed in a blister pack. The blister packs for each household were sealed in transparent protective outer bags. A bold warning was placed on each package stating that the medications inside were intended for homeland-security purposes, and should be opened only if and when instructed by authorities.

The Medkits were distributed to local residents belonging to three sociologically cohesive cohorts: first responders; the employees of certain corporations; and the clients of federally qualified health centers. Members of the participating households were given the Medkits and instructed on how to store them. The study households were then randomly assigned follow-up visits at two months, four months, and eight months – those periods were used to help determine if attitudes and/or behaviors changed over a carefully measured period of time.

During the follow-up visits, the participants were asked to retrieve their Medkits. When they had done so, they were given general preparedness kits – each of which

contained, among other things, a battery-powered radio and other non-pharmaceutical preparedness supplies to replace the original Medkit. The results were encouraging: 97 percent of the participants returned the Medkits at the end of the study; 99 percent of the returned Medkits had no pills missing; and 94 percent of the participants said they would like to have Medkits in their homes.

This may represent an entirely new approach to public health preparedness. If the public displays responsible behavior with such kits, it could reduce the reliance on PODs and other mass-prophylaxis approaches. It also raises a number of interesting questions, though, including the following: (a) Could anything other than antimicrobials be stored in such kits? (b) Could antivirals be provided in homes for pandemic influenza preparedness? (c) Or could radiological drugs be provided to those living near nuclear power facilities?

It is still too early, of course, to determine what the long-term policy implications of the St. Louis Medkit study might be. It seems safe to say, though, that the data provided by such studies may open new approaches to mass prophylaxis. This is especially true for those in the nation’s critical-infrastructure and special-needs populations, both of which may be difficult to reach during future times of crisis.

*Bruce Clements is a senior scientist and director of strategic development for Clean Earth Technologies LLC in Earth City, Missouri. He is responsible in those posts for developing and managing bioterrorism and emerging infectious disease research and intervention projects. A well known speaker and writer, Clements also serves as adjunct faculty at the Saint Louis University Institute for BioSecurity. His most recent book, *Disasters and Public Health: Planning and Response*, was released earlier this year.*

Questions of Preparedness

A Spring of Tragedy for Law Enforcement

By Joseph Trindal, Law Enforcement



This spring, tragedy struck the law-enforcement community in two major incidents – on opposite coasts. In March, the Police

Department of Oakland, California, was shaken by the slaying of Sergeants Mark Dunakin, Ervin Romans, and Daniel Sakai, and Officer John Hege, by a single assailant. The ambush murder – in Pittsburgh, Pennsylvania – a few weeks later of Police Officers Eric Kelly, Stephen Mayhle, and Paul Sciullo III was a historical first for that city. But multiple officer slayings usually *are* rare events.

Nonetheless, with the Pittsburgh slayings coming so soon after the Oakland shootout, it is logical to ask whether the two mass murders represent a disturbing new trend – for which most if not all U.S. law-enforcement agencies are ill prepared. A high-level examination of similar multiple officer slayings places the Pittsburgh and Oakland incidents in a slightly more understandable context. According to the Officer Down Memorial Page, the Oakland and Pittsburgh incidents contributed to a 13 percent increase in the number of officers already killed this year.

Emerging from the loss of police officers in line-of-duty incidents are a few overdue opportunities to assess and adjust law-enforcement tactics, training, and procedures against a real operating environment. Until this spring, the average length of time between nationally significant shooting situations has been anywhere from a few years to a full decade apart.

However, each such incident can and should become a watershed event – and an opportunity, therefore, to seek additional improvements in law-enforcement training and operations. For example, the Newhall shooting of 6 April 1970, in which four California Highway Patrolmen perished, became just such an event because it served as the foundation for new reality-

Emerging from the loss of police officers in line-of-duty incidents are a few overdue opportunities to assess law-enforcement tactics, training, and procedures against a real operating environment

based training and tactics when the nation's law-enforcement community at large quickly focused on providing officers better tools and techniques to improve survivability. Between Newhall and the next nationally noteworthy shooting, numerous law-enforcement agencies moved their tactics, training, and procedures several steps forward with the lessons learned from Newhall; the emergence of still relatively informal but increasingly effective information-sharing networks also helped.

Another Spring, Another Deadly Shootout

The next nationally publicized event also occurred in the spring season (May 1980), in California again, when several police officers confronted five heavily armed and determined bank robbers. Police training had clearly improved since Newhall, but the police officers were armed with .38 caliber revolvers and shotguns – but the robbers were better armed (with semi-automatic pistols, rifles, and improvised explosives). The May 1980 shootings, now better known as the Norco Shootout, led a number of additional police departments to rethink the option of having patrol rifles on the street rather than locked up in an armory somewhere.

Six years later, in yet another bloody spring, south Miami erupted in a fusillade of gunfire as the FBI initiated the arrest of another team of bank robbers. The 11 April 1986 shootout became a true watershed event in terms of lessons learned. Many law-enforcement agencies across the country finally retired the venerable revolver in favor of higher-capacity semi-automatic pistols. To meet the increased demand, the arms and ammunition industry developed a ballistic compromise between the 9mm and the .45 ACP that led to the .40 S&W used by most U.S. police agencies today.

The April 1986 tragedy, better known as the FBI Miami Shootout, also led to another national review of training and tactics and to the development and implementation of improved procedures to be followed in high-risk encounters. The key learning points developed from the Miami Shootout led to major improvements

in ballistics as well, and to greater emphasis on a survival mindset.

After Miami there also was less reluctance in the law-enforcement community to objectively studying the inter-dynamic confrontations between officers and assailants to distill other helpful lessons learned. Many local and regionally significant incidents were systematically studied in detail, with the results used nationally to influence training and develop more effective procedural standards. With more and more police departments learning to look at their responsibilities from a more global perspective, western law-enforcement agencies began sharing lessons learned with greater frequency and clarity.

The Waco Standoff And Political Repercussions

The spring of 1993 ushered in an unusual type of tragic situation. Just outside of Waco, Texas, federal and local law-enforcement personnel surrounded a well guarded compound in which heavily armed adults were living with other adults (unarmed) and a large number of children. The resulting, and politically controversial, Waco Shootout that followed a 51-day standoff is now viewed, however, as an atypical incident.

In contrast, the February 1997 North Hollywood shootout represented an all-too-familiar situation – a bank robbery gone awry. The robbers worked as a coordinated team, and their level of preparedness – in terms of weapons, protective equipment, and aggressive mindset – was unusual, but not totally unknown to law-enforcement personnel. The North Hollywood shootout was similar in many ways to the Norco Shootout 17 years earlier.

The two shooting incidents this spring are particularly disturbing, though, because each of them were single-assailant engagements in which initially responding and back-up officers were slain. A disturbingly common thread among nearly all of these notorious shootings has been the aggressive mindset of the

**Poplawski and Mixon
shared the mindset
of other notorious
police murderers –
an intense desire to
kill as many
law-enforcement
officers as possible,
regardless of their
own safety**

assailants involved. Driven by a fierce determination not to return to prison, Lovelle Mixon, the Oakland shooter, killed four officers in two separate firefights before taking his own life. The Pittsburgh incident, although different in other ways, also involved a single assailant, Richard Poplawski, who prepared for and ambushed the officers responding to a domestic-disturbance call.

Improved Protection Becomes a Two-Way Street

In both of this year's incidents, the assailant's speed and vicious aggressiveness contributed significantly to the lethal results. Speed and vicious aggression are, in fact, common assailant characteristics in many police officer slayings. Poplawski, though, apparently took several extra steps to prepare for the expected

police response. As Mixon did in the North Hollywood shootout, Poplawski wore ballistic-protection garments that enabled him to continue fighting while apparently unfazed, mentally or physically, by police handgun rounds.

Another significant factor worth considering: When Poplawski finally ceased his deadly attack, the only wounds he had sustained, it was discovered, were to his legs. He himself, though, was obviously aiming at the heads of the officers responding, seeking to avoid their ballistic-protection gear. Both Poplawski and Mixon shared the mindset of many other notorious police murderers – an intense desire to kill as many law-enforcement officers as possible, regardless of their own safety. Rarely do police encounter this high a level of murderous determination.

The Oakland and Pittsburgh police departments initiated investigations to determine if any additional lessons can be learned from the two shootouts. It seems likely that both investigations will reveal at least some correlations with previous incidents.

With respect to training, the spring of 2009 should underscore the need for police officers and trainers to emphasize practical understanding and rapid recognition of the viciously determined assailant. The rapid coordination of ad hoc teams of responding officers is essential to negate the advantages possessed by barricaded and viciously determined assailants. Large-scale incidents such as those mentioned above often bring together officers from different agencies – where rapid on-scene coordination is obviously essential but also becomes even more challenging.

In addition, as the Pittsburgh incident underscored, information sharing between sources on the scene – and through emergency dispatchers to responding officers – must be as complete and as timely as possible. Both of this spring’s shooting incidents will yield some new lessons learned and lead to additional best-practices recommendations. Oakland in particular has experienced relatively high tensions in the past between police and the communities they work in – and protect. If nothing else, there are or should be some new opportunities for police agencies and communities to use the healing process to strengthen bonds and develop a new unity against the common threat of violence that confronts both.

Joseph W. Trindal 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. A career federal law-enforcement investigator and executive, Trindal served with the U.S. Marshals Service for 20 years before accepting the position of director for the National Capital Region, Federal Protective Service, DHS. He has written numerous articles on integrative emergency management, and also authored the Technical Support Working Group Training Support Package entitled “Preparation for the Suicide/Homicide Bomber.” Trindal is presently serving as Director of the Critical Infrastructure Protection Division of Covenant Security International, a well established firm providing assessments, protection, security, and training across a broad spectrum of critical-infrastructure sectors.

Massachusetts, California, Montana, and New York

By Adam McLaughlin, State Homeland News



Massachusetts Hospital Tracks Swine Flu Via Twitter

HealthMap, the online disease-surveillance system created by Children’s Hospital Boston researchers, is getting faster. Now the real-time disease tracker is posting Twitter messages on the current swine-flu outbreak.

HealthMap already bolsters official reports with the early warning that Internet searches, chat rooms, or news stories can give about emerging infectious diseases. Sometimes these unofficial sources predate expert/official alerts, thereby serving as a potentially important asset when – as has already been demonstrated by the current swine-flu outbreak – diseases can quickly circle the globe via international air travel.

HealthMap added Twitter to its communications mix a month ago. As of 1 May the short-message service had increased from 50 to 1,800 users, most of them serving up “tweets” about cases from Lowell, Massachusetts, to New Zealand.

“I think that probably a lot of users coming to the site were specifically looking for that type of information – show me a list of the latest on this outbreak,” HealthMap co-founder Clark Freifeld said in an interview. “Twitter is ready to do that.”

HealthMap itself has been drawing 50,000 unique visitors a day, a level it used to reach in a month. Regular users include the World Health Organization, the U.S. Centers for Disease Control and Prevention,

and the European Centre for Disease Prevention and Control.

Informatics experts John Brownstein and Freifeld founded the service after the SARS outbreak in 2002. Brownstein reported in the March 2009 *Canadian Medical Association Journal* that Google searches for a food-borne disease spiked almost a month before the official announcement of some early cases (eventually linked to a Canadian deli meat plant), providing an early warning of the fatal outbreak.

When the online traffic about swine flu virtually exploded on HealthMap in late April, the system tracked the earliest mention of the disease back to a 1 April report in a local newspaper in Veracruz, Mexico. “The reality is we are combing through hundreds of outbreaks at the same time,” Brownstein commented. “Avian flu in Egypt was a major concern then, so we were following it more closely.”

More cases emerged throughout the month, bringing swine flu into the same WHO category as SARS and an earlier outbreak of avian flu: an outbreak of international significance.

California LAPD Opens New Harbor Division Police Station

The Los Angeles Police Department unveiled its new \$40-million police station last week during a 25 April ribbon-cutting ceremony for its Harbor Station, which serves parts of San Pedro, Harbor Gateway, and Wilmington.

The 50,000-square-foot facility is the new home of the Harbor Division’s

Is Your Membership About To Expire or Has It Expired?

If YES, then visit www.DomesticPreparedness.com

Enter Promo Code: **RENEW**

to extend your subscription today!

Qualified members receive complimentary subscription

260 patrol officers, detectives, and support staff, who had been working out of temporary trailers since 2005, when the nearly century-old Harbor Station was closed for demolition. The replacement station was built with money from Proposition Q, a \$600-million bond initiative approved by voters in 2002 to improve public-safety facilities in general.

There will be no increase in staffing, but the new facilities – which include a 300-inmate jail – are expected to make operations more efficient, said Lt. John Pasquariello. Because there was no jail at the temporary site, officers have had to drive prisoners to the 77th Division jail, 20 minutes away, taking them off their regular beat for extended periods.

The new station on John S. Gibson Boulevard includes a helicopter pad, parking structure, and garage. What is now a small, cacophonous lobby will be replaced by a more spacious one with ample seating and a community room. The division's uniformed and civilian staff, and local citizens, were lavish in their praise about the upgrading. "I've been very surprised at how much it means to the community," said Michele D'Angelo, a civilian employee of the Harbor community-relations section since 1995. Her fellow employees are "delighted and happy with the architecture," she said.

"Everybody knows about it," Pasquariello added. "It is right next to the Harbor Freeway, and they have been watching it go up for several years."

Montana Explosion Exercise on Montana State U Campus

It was not a real emergency, but it was a good decision to prepare

now in case there is one in the future. Emergency responders converged on Leon Johnson Hall at Montana State University (MSU) in Bozeman shortly after noon on Monday, 11 May, following a call that there had been an "explosion" on the building's sixth floor. The pre-scripted call started the exercise that would allow emergency responders to test the response plan developed for Leon Johnson Hall, an eight-

When the online traffic about swine flu virtually exploded on HealthMap the system tracked the earliest mention of the disease back to a 1 April report in a local newspaper in Veracruz

story building that houses various MSU offices as well as a number of laboratories designed for research and testing in such varied fields as the plant sciences, land resources and environmental sciences, chemistry/biochemistry, and entomology.

MSU campus emergency services and Bozeman police and fire personnel, along with a hazmat trailer, responded to the simulated explosion. A command center was quickly set up outside the building in accordance with the exercise plan.

The 911 call reporting the explosion was made at about noon. The exercise plan included scanner reports indicating: (a) that simulated flames

were shooting from the building's sixth floor; and (b) that the building had been evacuated.

The emergency-responder response time was quick: about two minutes, according to authorities. Responders evacuated about 20 to 30 staff members, two with injuries and a trapped person in a wheelchair.

Tracy Ellig, director of the MSU News Service, noted that there are not many places in Bozeman where a high-rise drill could be conducted. "And [such drills] are very valuable ... because it [otherwise] would be an extremely complicated situation." Having the "opportunity to exercise," he said, "is going to be good for both Bozeman Emergency Services and the university."

Responders said they had intentionally scheduled the drill for a time when classes had finished up for the semester and graduation had taken place, making the campus much quieter than it had been previously.

New York NYPD Breaks Up Identity Theft Ring

On May 15, New York City officials announced that the New York Police Department (NYPD) had broken up a sophisticated identity theft ring that ruined the credit of an estimated 6,000 victims and bilked banks out of \$15 million in bogus charges.

The scam, which stretched from New York to Nigeria, is one of the largest operations of its kind ever dismantled by the NYPD, Police Commissioner Raymond Kelly said.

The thieves somehow managed – the investigation is still ongoing – to get their hands on thousands of

credit cards legitimately issued in the victims' names, and had intercepted the cards before they arrived at their proper destinations.

The thieves then called the credit card companies – using a legal device called a SpoofCard to disguise their own voices and phone numbers – to activate the stolen credit cards. “From a law-enforcement perspective, such cards are anything but a spoof,” commented Queens District Attorney Richard Brown.

When the companies fell for the ruse, the suspects used the cards for cash advances and/or to buy high-priced luxury items in Japan, Saudi Arabia, and Dubai. They even paid, in some cases, to increase a card's line of credit so they could use it again for additional cash. In addition, after the maximum purchase limits of some cards had been reached, the thieves recycled the cards as backup identification to open new credit accounts.

The card thefts were discovered not quite two years ago when a Queens realtor opened a package meant for one of his employees and found 60 credit cards – the type “normally issued in anticipation of a customer's card expiring,” Kelly said.

The NYPD traced those cards around the globe. During a 21-month investigation, the department used 80 phone taps to eavesdrop on more than one million calls, according to Deputy Chief Jeremiah Quinlan, head of the NYPD's special investigations division.

Investigators fluent in West African languages and dialects were called in to “tease out” 250,000 conversations relevant to the probe. Eventually, 35 suspects, most of them Nigerian immigrants living in the city, were

arrested and now face charges of enterprise corruption, larceny, and conspiracy. After the scheme came to light, the banks became responsible for the stolen money, but the intended cardholders still have to rebuild their now ruined individual credit ratings.

Police are still trying to figure out exactly how the suspects obtained the

cards, said Deputy Inspector Gregory Antonsen, head of the NYPD's ID Theft Task Force.

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.

EXPOSE CHEMICAL HAZARDS



AP4C

HANDHELD CHEMICAL ALARM DETECTOR

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



ADVANCED SPECTRO-PHOTOMETRY DETECTS

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

PROENGIN

www.proengin.com

(954) 760-9990
e-mail: contact@proengin.com