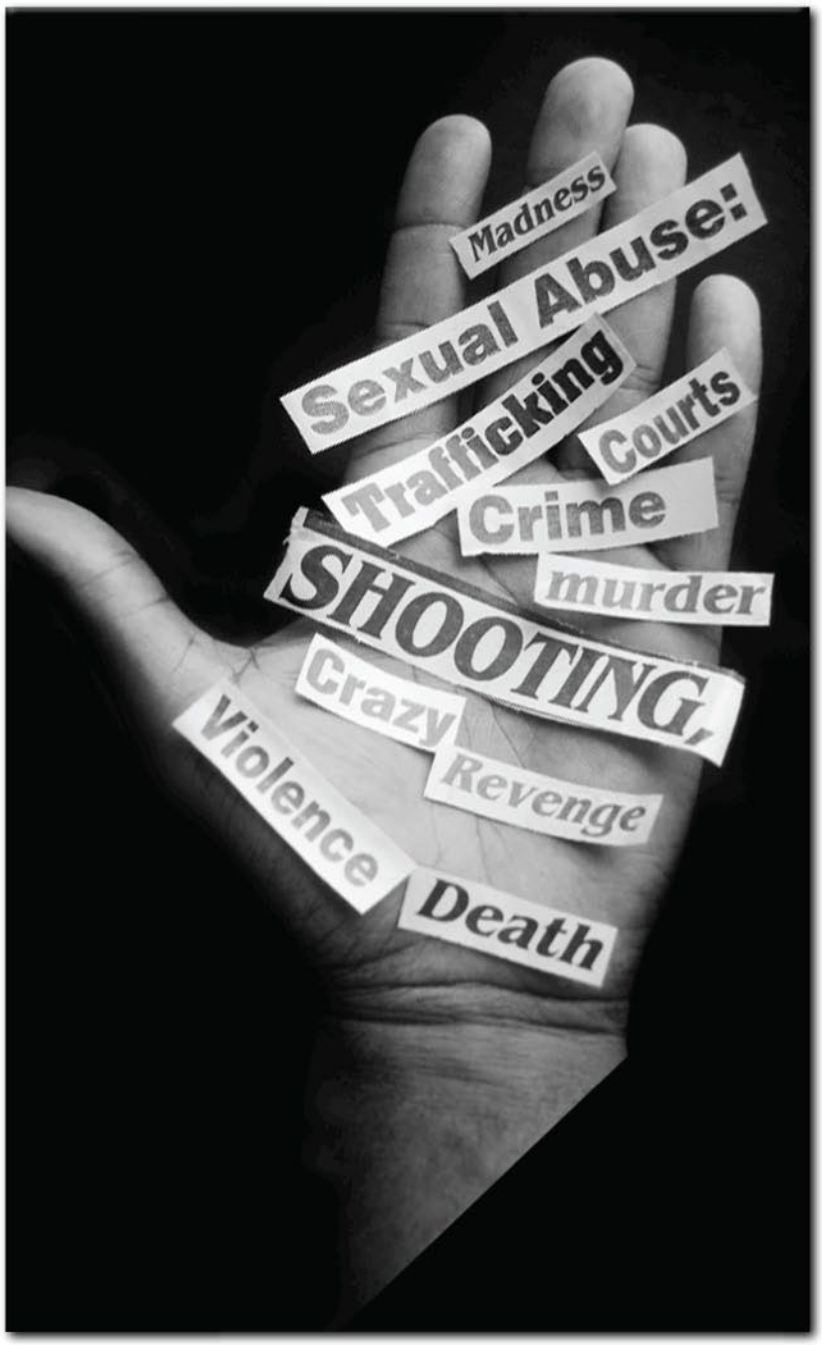
domestic preparedness .com

DomPrep Journal

US Annual $100 Volume 9 Issue 3, March 2013

Violence



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

Staff
Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

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

Catherine Feinman
Editor
cfeinman@domprep.com

Susan Collins
Director, Production & Strategic Execution
scollins@domprep.com

Derek Sharp
Manager of Business Development
dsharp@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

John Morton
Strategic Advisor
jmorton@domprep.com

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

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 Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher.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

Editor's Notes

By James D. Hessman

In the 21st Century, advances in technology, communication, transportation, and training can – and often do – facilitate the criminal activities of persons intending to do harm. However, those same advances also offer opportunities for everyone – not just police officers, but people from every discipline including private citizens and even children – to play a part in counteracting, thwarting, and protecting themselves from such activities.

The thirteen knowledgeable experts contributing to this month's printable issue of *DPJ* examine various aspects of the important topic of violent crimes, and agree on a few general principles. Although there is no solution to prevent every crime, they do offer several recommendations on how to deter criminals, protect innocent victims, and prepare local communities, as well as entire nations, to prevent at least some of the destruction and death.

Tracy L. Frazzano and G. Matthew Snyder lead the issue with a thoughtful analysis of the increased complexity of modern crimes. Whether working alone or in small groups, individual assailants armed with a mixed bag of weapons have the ability to attack multiple targets of opportunity and kill many people in a brief period of time. Joseph Trindal describes one such crime that occurred in Algeria, in the northwest corner of Africa, where a well organized group of terrorists attacked the In Amenas Gas Refinery less than three months ago, killing not only those who tried to escape but also some who willingly surrendered. Donald J. Cymrot and Stephen E. Rickman suggest ways to better protect schools and children from attacks similar to the one in Newtown, Connecticut, less than four months ago.

Michael J. Pitts focuses special attention on the April 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City to emphasize the importance of situational awareness. Richard Schoeberl contributes a true insider's report on the violence along the U.S./Mexican border – and the debate over the "spillover" effect of increased crime on the American side of the border. Jeffrey D. Simon addresses the dilemma of dealing with "lone-wolf" terrorists: Theodore Kaczynski, the so-called Unabomber; Norwegian mass murderer Anders Breivik; the Columbine and Virginia Tech shooters – the list could go on and on.

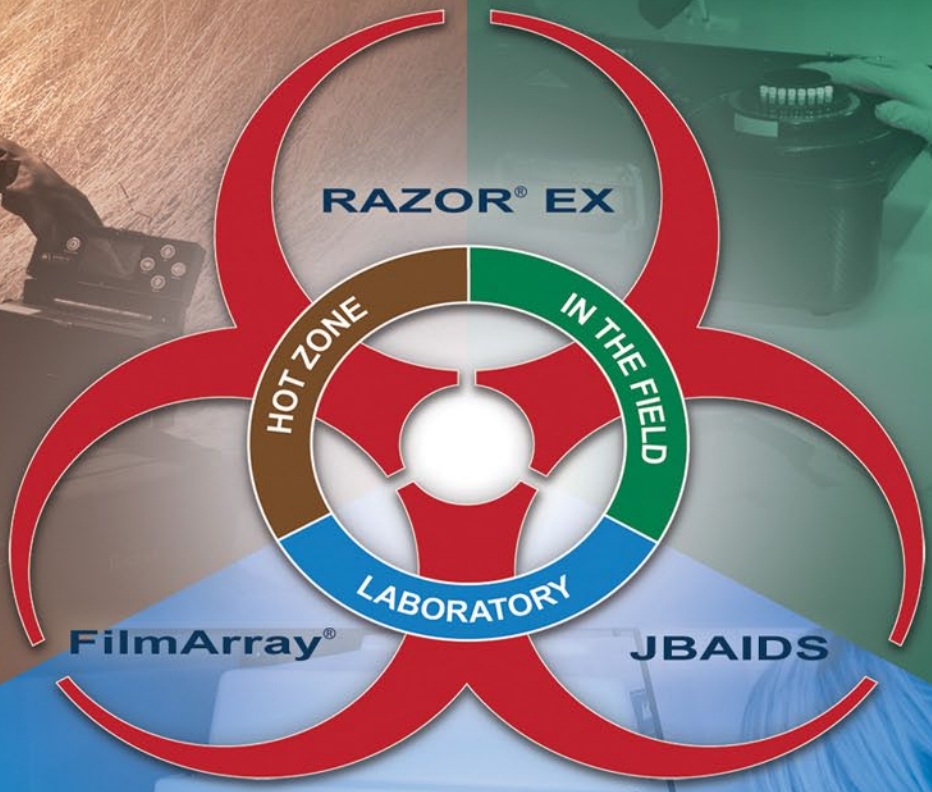
There are a few common-sense things that can, in fact, be done to at least slow down and maybe reduce violent crimes significantly. Monica Giovachino stresses the need to focus early on the improvement of law enforcement officer safety. Glen Rudner discusses "scene security" and how to obtain it from the firefighter's perspective. Rodrigo Moscoso adds an optimistic note with his report on the use of improved technology to enhance what is known as "predictive policing." Joseph Cahill emphasizes the ongoing need to stay ahead of the game through long-range planning, constant and effective training, and always being fully prepared for the unforeseen/unforeseeable as well as likely dangers and difficulties. Shannon Arledge rounds out the issue with a special report on several of the no-/low-cost training courses available to first responders at the FEMA Center for Domestic Preparedness in Anniston, Alabama.

About the Cover: Crime and violence come in many forms, through a variety of methods (or combination thereof), at the hands of many people – from lone wolves to large terrorist cells. How to respond to the many possible scenarios is not black and white. It requires careful planning, preparation, and training. (iStock Photo)

BioSurveillance

Flexible, Accurate, Proven Ready

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



Idaho Technology is now

BIOFIRE DIAGNOSTICS, INC.

Discover the system for your mission.

WWW.BIO-SURVEILLANCE.COM

Hybrid Targeted Violence: Fire, Firearms & Complex Threats

By Tracy L. Frazzano, with G. Matthew Snyder, Law Enforcement

Attacks involving firearms, explosives, or even the use of fire as a weapon against unsuspecting victims can quickly strain the capabilities of most first-responder agencies. When an attack involves multiple adversaries and several modalities of violence, however, the difficulty rises exponentially. In today's increasingly dangerous world, preparing for the next complex incident may well require a more descriptive term that goes beyond such common phrases as "active shooter" or "terrorist attack."

These terms no longer adequately describe the grim realities of the more complex threats occurring more and more frequently in recent years, not only in the United States but in many other countries as well. A more comprehensive term for today's complex attack scenarios is perhaps needed – "hybrid targeted violence" (HTV) is one example of such a term that, if generally accepted, could be defined as "an intentional use of force to cause physical injury or death to a specifically identified population using multifaceted conventional weapons and tactics."

That term, which more accurately describes the operational range of the broader modern spectrum of dangers confronting first responders today, encompasses both "hybrid" weapons and diverse tactics. The numerous HTV assaults that have been launched in recent years used not only a combination of lethal conventional weapons – fire, small arms, and improvised explosive devices (IEDs), for example – but also a diverse set of well-planned tactics such as ambushes, breaches, barricades, and maneuvers.

From Rome to Mumbai to Aurora & Beyond

Diversionary tactics are not new, of course – the Roman legions used them in numerous campaigns. The use of a broad spectrum of weapons of various types, if available, also has been a standard operating procedure throughout history. The difference today is that a single or very small number of terrorists who have access to weapons of various types pose a considerable danger to communities in a free society. They also have the benefit of greater mobility and instant communications, which makes them that much harder to stop.

The coordinated November 2008 attacks in Mumbai, India, by ten armed militants is perhaps the best recent example of how a small but well-organized team can terrorize an entire nation. During the three-day siege, the militants divided into small teams to carry out a carefully crafted and orchestrated series of attacks. Lobbing grenades and firing assault rifles, they entered several hotels, a crowded railway station, and a

number of other buildings, killing at least 164 people and injuring more than 300 others. The siege was so devastating and so effective that it, along with current threat intelligence, served as the foundation of a tabletop exercise in the United States sponsored by the U.S. Department of Homeland Security, the National Counterterrorism Center, and the Federal Bureau of Investigation.

There have been many other mass-killing scenarios in recent years. Two young men, using both IEDs and firearms, carried out the 1999 Columbine High School attack that killed 12 students and one teacher, and injured 21 other students – and today, 14 years later, continues to impact school safety and law enforcement response protocols. The 2012 ambush of firefighters in Webster, New York, which killed two people and injured two more, represents the significant harm that one man can levy – with fire being used as both a weapon and a distraction – to maximize the effectiveness of a small-arms assault. Another contemporary example of a complex hybrid attack is the 2012 Aurora Theater shooting in Colorado in which one man – armed with chemical weapons, IEDs, and firearms – was able to single-handedly kill 12 people and injure 58 others in a very short period of time.

As terrorist tactics change, so too must the terminology used to comprehensively describe and prepare for such attacks. "Hybrid targeted violence" perhaps best encapsulates the threat posed to today's first responders.

These and other headline incidents of similar magnitude are grim reminders that complex manmade events can occur in any jurisdiction, at any time – and with little or no warning. The men and women in public safety and emergency response positions who are on duty when such events start – and then unfold in many and various unexpected ways – must therefore be cognitively prepared both to neutralize the attacker(s) and to protect the lives of the targeted population.

JCTAWS: A Paradigm Shift in U.S. Training Tactics

Since 2011, the Joint Counterterrorism Awareness Workshop Series (JCTAWS) – sponsored by the Federal Bureau of Investigation, the Department of Homeland Security, and the National Counterterrorism Center – has been a collaborative effort among federal, state, local, and private-sector agencies and organizations that empowers cities to provide significantly improved responses to a HTV incident. The JCTAWS HTV scenario focuses special attention on the use of cooperative response strategies well ahead of time, rather than during an actual event. These ongoing workshops reveal not only current strengths but also the need for improvement in certain areas. The latter weaknesses, of course, are best identified in a training environment, rather than in an active-shooter incident.

A major value-added benefit of the workshops is that they bring together representatives from all levels of the federal, local, tribal, state, and territorial partners, as well as some nongovernmental organizations, to address and defeat a complex threat. Although a single complex attack may quickly overwhelm almost any community, it can be defeated – but not without considerable difficulty and, perhaps, many casualties. The potential launching of several simultaneous attacks, carried out by multiple attackers, poses a much greater danger, though – and requires that first responders join forces, in advance, to perfect a rapid response strategy that embraces a "whole community" perspective on cooperation and collaboration.

A Turbulent Future Requires a Greater Sense of Urgency

Changing the current perspectives of first responders to recognize a potential HTV incident can positively influence training, tactics, and the development of new procedures that build resilient team approaches. The goal is clear: The nation's future HTV response capabilities should be both expanded and fortified to the point that defenders and responders can swiftly and decisively disrupt the Mumbai, Columbine, and Newtown types of attacks that have killed so many innocent people and captured the attention of the nation, and the world, in recent years.

Forums such as the JCTAWS workshops are particularly effective for brainstorming innovative strategies across functional disciplines through informative and cooperative discussion-based drills and exercises. Nonetheless, the only "appropriate" time to debate precisely how police, fire, and medical professionals should engage an active shooter in a burning building – while also caring for the injured – is in training sessions, rather than after human blood has been spilled during an actual attack.

In short, whole community shifts in thinking are essential to achieve both strategic and tactical success against an ongoing threat. Predicting the next community likely to be subjected to an HTV attack is virtually impossible, but there is a high degree of certainty that such an attack will, in fact, occur again – perhaps many times, and in many locales.

It is up to the strategic leadership of the nation's public safety community to prepare, fully and well in advance, the interdisciplinary teams needed to thwart future HTV incidents, upon which they and their agencies will be judged by for many years to come. The lives of all members of the local community depend on creation of a collective sense of urgency across all functional domains of the public safety community.

Tracy L. Frazzano, a Lieutenant with the Montclair Police Department in New Jersey, was awarded the 2011 Center for Homeland Defense and Security Alumni Fellowship and detailed to the U.S. Department of Homeland Security's Federal Emergency Management Agency in Washington, D.C., for one year. A 2010 graduate of the Naval Postgraduate School in Monterey, California, she earned a Master of Arts degree in security studies (homeland security and defense), and also holds a Master of Arts degree in human resources training and development, from Seton Hall University.

G. Matthew Snyder is an advanced leadership instructor with the U.S. Department of Homeland Security. A police officer with the City of Waynesboro (Virginia) Police Department since 1992, he now serves as a part-time investigator assigned to the department's Criminal Investigations Division. In 2010, he retired from the U.S. Army Reserve as a Command Sergeant Major with over 24 years of active and reserve service. He earned a master's degree in public administration from James Madison University and recently completed his coursework for a doctorate in education at Liberty University.

Note: The opinions of the authors are their own. They do not represent the official opinions of their respective organizations.

Improving Officer Safety Through Preparation & Practice

By Monica Giovachino, Law Enforcement

Although the U.S. Incident Command System (ICS) has existed for four decades, analyses of real-world incidents and exercises show that many of the nation's law enforcement agencies still struggle to establish and use an effective incident command process during particularly complex events, such as active-shooter situations.

Fire agencies initially developed and implemented the ICS concept to help manage multi-agency responses to wildfires. Because its common terminology and scalability helped responders from other organizations integrate into an effective incident management structure, many public safety agencies adopted the ICS model for their own purposes. Since being incorporated by the U.S. Department of Homeland Security (DHS) into the federal government's National Incident Management System (NIMS) in 2004, ICS-related guidelines and training processes have become more readily available to a broad spectrum of other first-responder agencies and organizations.

During active-shooter incidents and other complex situations, law enforcement officers must decide if and when to establish an incident command post. Those decisions affect the safety of everyone on and around the scene.

Baltimore, Las Vegas & Oakland: Three Deadly Examples

Nonetheless, the consequences of not establishing and using an effective incident command system can be tragic. In December 2009, for example, an Independent Board of Inquiry cited the lack of command and control as a key factor contributing to the deaths of police officers during a 2009 incident in Oakland, California.

The incident began when two officers were shot during a vehicle stop. The Inquiry Board stated that the command officers responding failed to recognize the event as a complex incident and, largely for that reason, did not establish an incident command post. One operational result was that there was little or no control of other personnel responding to the incident. Moreover, the Board also said, no formal processes had been established for planning, communications, and/or sharing information. Nearly two hours after the initial shooting, two more officers lost their lives when they engaged the suspect at his apartment building.

In 2011, an Independent Review Board examining a police-involved shooting in Baltimore, Maryland, determined that the failure to establish an incident command post contributed to an officer's death. When Baltimore police officers arrived at a local nightclub to assist with crowd control and dispersal, they encountered disorderly conduct and radioed for any units available to respond and assist. Although many officers did in fact respond, they were not formally tasked or managed because an incident command post was not established. The increasingly chaotic situation not only jeopardized officer safety in general but also directly resulted in the death of a plain clothes police officer.

More recently, a 2012 analysis of police-involved shootings in Las Vegas, Nevada, revealed a similar situation. The study found that tactical errors and fatalities are in general more prevalent in situations in which four or more officers respond to a scene. The police agencies specifically involved in such situations had policies in place related to incident command, and some training requirements as well, but the overall guidance the agencies provided had not been effectively integrated into the department's daily operations and overall "culture."

Practicing & Tailoring ICS for Law Enforcement Operations

When assessing any situation, regardless of scale, it is critical that law enforcement officials consider and implement the incident command policies needed to

manage the response. Fortunately, the flexibility provided by the federal government's ICS guidelines makes them adaptable to almost any situation imaginable. Even so, the December 2012 tragic shooting of grade-school students (and school staff members) in Newtown, Connecticut, and the February 2013 shooting spree by a former Los Angeles, California, police officer vividly illustrate that active-shooter situations can occur either suddenly without notice or be preceded by information that provides some warning.

Time is another ambiguous factor that must be taken into consideration. Certain incidents may last only a few minutes; others, though, might evolve into extended manhunts that span several days or even weeks. However, as the complexity of an event increases – for example, an attack involving multiple adversaries and weapons, similar to the three-day November 2008 attacks in Mumbai, India, that killed 164 people and injured more than 300 others – the ICS structure can quickly expand to include several area command posts reporting to an incident's unified command center.

However, regardless of how experienced and well trained an individual officer may be in adapting ICS guidelines when responding to a dangerous incident, planning and preparation at the department level also helps considerably to ensure mission success. One nonviolent example occurred in Tampa, Florida, where the police department gained extensive experience in using ICS guidelines to help ensure public safety when the city was preparing for the 2009 Super Bowl.

Because of its conscientious preparations and frequent practice drills, the Tampa Police Department was later able to follow the same ICS-type guidelines immediately after a 2010 shooting of two police officers during a traffic stop. The massive manhunt that followed lasted 96 hours, involved more than 1,000 personnel from 22 law enforcement agencies, and ended with the capture of the suspect.

The ability to effectively use an incident command structure in a complex situation, however, requires advance planning, focused training, and repeated practice and assessment. The following examples are just a few of the more important steps various responder agencies can and should take to tailor the ICS concept for their own operations:

- Develop agency-specific policies and procedures that outline the ICS structures needed to cope with both high-risk and common scenarios;
- Integrate these same policies and procedures into current training drills and exercises – the use of scenario-based training for active-shooter situations, for example – rather than relying on general ICS course content;
- Coordinate ICS planning, training, and exercises with partner agencies and organizations that are likely to participate in future response operations;
- Use ICS for managing special events and other non-emergency incidents to gain additional experience and facilitate the use of ICS guidelines in normal police operations; and
- Continually assess operations through exercises and analyses of real-world incidents – and follow up by updating, as and when needed, current policies, procedures, and training to address and rectify any problematic issues that become evident.

In short, through deliberate and focused planning and preparation, as well as continuous assessments and improvements, the nation's law enforcement agencies can significantly maintain their readiness to implement the ICS policies and plans needed to achieve response objectives and maximize officer safety.

Monica Giovachino is a managing director in the Safety and Security Division at CNA, where she has been employed since 1994. She has special expertise in the design and evaluation of complex exercises and in the evaluation of real-world events. She also has: (a) led the evaluations of a number of "TOPOFF" (Top Officials) Exercises and National-Level Exercises scheduled for the U.S. Department of Homeland Security; (b) managed numerous other exercise programs for various local, state, and federal agencies; and (c) led the analyses of several complex real-world operations. Included in the latter category were evaluations of responses to hurricanes, disease outbreaks, chemical/biological "events," and law enforcement incidents.

Enhancing Zones to Protect the Emergency Responder

By Glen Rudner, Fire/HazMat

Although the concept of armed persons targeting responders is not new, several 2012 lone-shooter incidents – at a movie theater in Aurora, Colorado; at an elementary school in Newtown, Connecticut; and at a house fire in West Webster, New York – have raised greater concern among emergency responders for personal safety when arriving on scene. Specifically, on 24 December 2012 in West Webster, four firefighters were shot – two mortally wounded and two others injured – when responding to a fire that was deliberately set by the gunman. That incident, among others, raises concerns not only about the security of the scene itself, but also the security of the overall response efforts.

By incorporating the inner and outer perimeters set by law enforcement, the responder community could better protect the fire, emergency medical services, and hazmat personnel at the scene of an incident.

Response & Scene Security

Based on the type of incident, fire, emergency medical services (EMS), and hazardous materials (hazmat) teams should consider reworking standard operating procedures and guidelines for developing a secure zone around operational areas. Reviewing and, if necessary, updating the procedures and guidelines will ensure that the teams have enough room to handle all operations on scene with minimal fear of attack. Areas of concern to consider include:

- People management – limiting the number of required responders within each of the designated working zones and ensuring that there is someone guarding the scene as operations continue;
- Personal protective equipment (PPE) – purchasing and regularly using the best level of PPE (although many departments have body armor to protect personnel in high-risk/high-crime areas, this may not be the best solution or an appropriate response for fire, EMS, and hazmat teams); and
- Information sharing – transmitting sufficient information from the dispatching agencies to the emergency responders who will be on the scene.

Zones & Perimeters

After addressing concerns about people management, PPE, and information sharing, emergency responders then should consider integrating the fire and EMS "zones" (hot, warm, and cold) into the law enforcement "perimeter lines" (inner and outer). Traditionally, fire, EMS, and hazmat teams use three zones to define the safety areas of an incident, but they do not always take in to consideration the two perimeters that are defined and used by law enforcement.

The three zones include: (a) The "hot zone," where the release, problem, and/or hazard are located; (b) the "warm zone," where decontamination, equipment staging, etc. occur; and (c) the "cold zone," where the command post is located, personnel are staged, and other activities that do not require any specialized equipment are performed. Unfortunately, that is where the incident perimeter ends for the fire, EMS, and hazmat services, but even the cold zone is still in fact considered by the law enforcement community as part of the "inner perimeter." The "outer perimeter" then offers a "buffer" zone for the incident scene and a protective area for emergency responders, as well as areas for other incident-related needs – for example, rehabilitation, equipment staging, and additional support staff.

Communicating & Working Together

There has been a tremendous amount of discussion and progress since the events of 9/11 with regard to interoperability. More than just a term for synchronized radio communications, "interoperability" also means that the multiple agencies that respond to both

minor and major incidents must be able to speak to each other and work together for the good of the community. When an incident occurs, emergency responders should ask for and provide sufficient information, carefully determine the type of response needed, and establish an open line of communications with law enforcement personnel as they determine the needs and set the limits of the outer perimeter.

Today, many law enforcement agencies respond to most, if not all, of the same incidents that require fire, EMS, and hazmat responses. At the scene of an incident, law enforcement personnel can provide tremendous resources – including intelligence and more importantly protection – to other first responders.

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

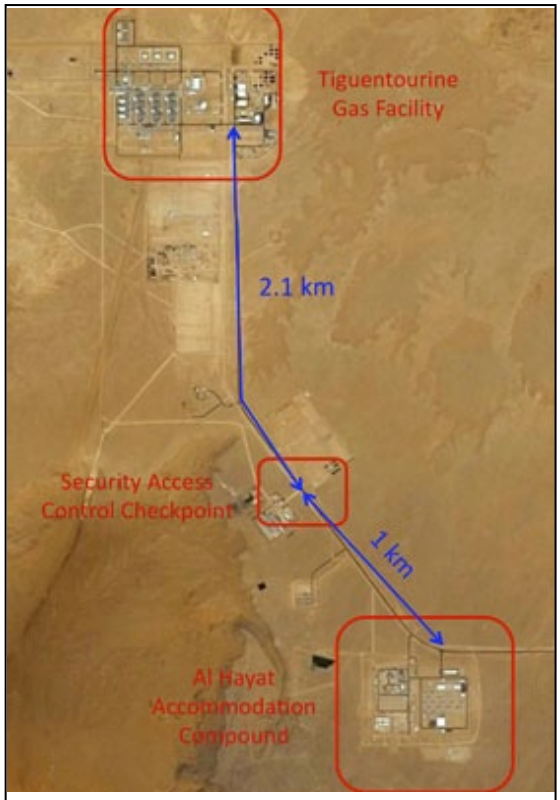
Gas Refinery Attack in Algeria: The Lessons Learned

By Joseph Trindal, Building Protection

In the early morning hours of 16 January 2013, a coordinated band of terrorists attacked a convoy of gas refinery workers as they departed the housing area of the In Amenas Gas Refinery in eastern Algeria. The attack was described in a 25 January 2013 article – in *Chronicles: A Magazine of American Culture* – as the "most elaborate" to date on the African continent. Targeting critical infrastructure, the In Amenas attack is considered to be equivalent to India's energy-sector incident in November 2008, which included a coordinated attack, hostage-taking, and three-day siege in Mumbai. The Algerian incident led to a four-day siege resulting in the deaths of 38 hostages.

The Situational Environment

The In Amenas Gas Project is a multinational joint venture and the largest production wet gas facility in Algeria. The Tiguentourine facility, which is only 50 miles from the Libyan border, processes over nine billion cubic meters of natural gas annually. The desolate In Amenas area of Illizi province is also 717 miles from the population center of Algiers. According to Sonatrach, Algeria's state-owned petrochemical company, more than 700 workers are assigned to the facility.



The condition of the In Amenas Gas Refinery at the time of the attack.

Among the workers present on 16 January were over 130 foreign nationals and expatriates from Norway, Japan, England, the United States, and several other countries. The site's geographic isolation, which delayed response forces, coupled with the presence of large numbers of western workers, favored the terrorists' objectives.

The region has experienced decades of terrorist activity as part of the Islamic Maghreb effort to establish an Islamic caliphate across northwestern Africa. Struggles with Islamic radicals in Algeria, often referred to as the "gateway between Europe and Africa," boiled into civil war in the 1990s. In 2006, after a period of deescalating tension, al-Qaida formally joined forces with the Salafist Group for Preaching and Combat, also known as the Groupe Salafiste pour la Prédication et le Combat (GSPC).

In 2007, the solidified group became known as Al-Qaida in the Islamic Maghreb (AQIM). According to Algerian government sources, Algeria, a former French colony, experienced nearly 200 attacks each year in 2011 and 2012, the majority of which targeted military and police as well as western workers and tourists with bombings, ambushes, and kidnappings. Algerian counterterrorism efforts produced encouraging results in 2012, and helped to foster the expansion of foreign investment in energy production. That same year, though, Mali – a small country southwest of Algeria – cascaded into civil war as insurgent forces swept toward the country's capital of Bamako resulting in French military intervention.

An Attack "Signed in Blood"

Late in 2012, plans and preparations were underway for an AQIM attack in Algeria targeting multinational-owned, critical infrastructure with easy access from safe-haven terrorist bases in Libya. According to a 21 January 2013 article in *MacLean's* magazine, Algerian sources reported that at least one of the attackers had been a driver at the facility; an indication of insider-sourced pre-attack intelligence used in planning. The "Signed in Blood Battalion" – a self-named

sub-group of the AQIM that is commanded by and under the operational command of Mokhtar Belmokhtar – launched the attack with a heavily armed team of 33-40 terrorists.

Two Canadian citizens were members of the attack team, according to Algerian sources. In addition, the terrorists convoyed from Libya, under the cover of darkness, in as many as nine Toyota vehicles disguised with markings resembling those on Sonatrach company vehicles. The terrorists, who were armed with AK-47 rifles, PKM variant machine guns, RPG-7 grenade launchers, and an array of explosives, first ambushed an escorted convoy of buses carrying workers departing along the single access road from the gas plant's Al-Hayat housing complex, which is about 1.5 miles from the main plant. The terrorists then proceeded to neutralize the plant's security checkpoint with small arms fire – but not before Mohamed Lamine Lahmar, a security guard later killed in the engagement, had activated the plant's distress alarm. The terrorists then divided into several assault teams, executing coordinated operations against the Al-Hayat complex and the Tiguentourine processing facility.

The Algerian forces closing in on the kidnappers - 19 January 2013

At both locations, word spread quickly as workers responded to the piercing alarm, coupled with the information that they were under attack. Thanks to the early warning and to the quick thinking of many workers who adhered to the site protocols governing responses to terrorist attacks, some were able to escape or hide. Other workers in the plant's process control room began shutting down processing units and gas feed valves; these actions also were consistent with the plant's protocols for responding to alarms. As the terrorist assault continued, survivors later reported, electricity was being shut down throughout the site.

The survivors also reported that the terrorists started to collect and segregate the hostages into small groups. Unlike the relatively compressed ground areas in other hostage takeovers – the 2002 Beslan school attack in Ingushetia, Russia, for example, and the Dubrovka theater attack in Moscow that same year – the In Amenas Gas Refinery is a sprawling complex covering slightly over five square miles. The plant's workers, supported by a modest security force, are scattered throughout the entire area.

In addition to the elements of surprise and overwhelming force, the survivors also reported that the terrorists used both ruse and deception – coercing some hostages, for example, to lure hiding workers into the open. Some of the hostages were summarily executed, regardless of their compliance with terrorist instructions. Most of the Algerian workers and Muslims were released, but some non-Muslim foreigners were not only retained but also were fitted with collar and belt bombs.

As the terrorists consolidated their control over the facility, the hostages were dispersed to various holding locations throughout the complex. According to at least some reports, the terrorists also rigged: (a) victim-operated improvised explosive devices (VOIEDs) and/or other booby traps at key access points; and (b) various other explosives at key processing locations (in an apparent effort to ultimately detonate the entire site).

The Response

Algerian forces started their response within a couple hours after the attack started, but the remote location of the plant delayed the arrival of any sizable counterterrorist force during most of the first day. The remote location of the plant and complexity of the attack also made a situational size-up and the collection of ground truth intelligence more difficult. During the first night, however, the first Algerian forces arriving started to contain the site.

Very early on the morning of the second day, a group of about 45 survivors escaped on foot from the Al-Hayat complex into the desert. According to Alan Wright, a 37-year-old health and safety advisor at the In Amenas refinery, he and the other survivors were intercepted in the desert by armed personnel, but were not sure if the latter were terrorists or government response personnel. They were relieved to learn that they were government forces, who were themselves not sure of the identities of the people running toward them in the desert. Also early on the second day, Algerian helicopter gunships engaged and neutralized two vehicles travelling along the only access road away from the Al-Hayat complex. It was later reported that the vehicles were carrying both terrorists and hostages. Other workers escaped in various ways during the siege.

As the world's attention became increasingly focused on the In Amenas hostage crisis, Algerian forces cleared and secured the Al-Hayat complex and security checkpoint, consolidating the government's containment of the Tiguentourine processing facility. Communications between the hostage takers and government forces were unproductive and the terrorists escalated the situation by threatening to detonate the plant if a rescue operation were attempted. During the siege, AQIM announced two demands: (a) The cessation of French operations in Mali; and (b) the release of two prisoners being held in the United States: Sheikh Omar Abdel-Rahman and Pakistani scientist Aafia Siddiqui.

Finally, on the fourth day of the siege, amid sporadic exchanges of gunfire with the terrorists, Algerian forces reported that, because of information about hostages being executed, government troops had started a rescue assault to regain control of the Tiguentourine facility. Participating in the counter-attack were a coordinated force of ground and air units – some of them in Russian-built T-72 battle tanks and armored personnel carriers – and special forces personnel on foot.

According to Algerian government officials, an unspecified number of the 38 hostages killed were found to have died of a single shot to the head, supporting government and survivor reports of hostage executions. In addition, an explosive was detonated next to one of the processing units, but failed to cause much damage, thanks to the early mitigation measures taken by plant workers on the first day of the siege. Other explosives also were found at various locations throughout the site, indicating that a major sabotage effort was planned but not fully carried out.

Lessons Learned

The Refinery attack was in many respects a true watershed event because it demonstrates the will and ability of terrorist groups to plan and execute attacks on very difficult and even remote critical-infrastructure targets. Following, based on the lessons learned from this incident, are some important actions that should be considered to help strengthen risk awareness and also to reassess current response capabilities:

- *Improve Predictive Intelligence Analysis Capabilities* – It has been reported that intelligence analysis of the regional, national, and site-specific threat dynamics of eastern Algeria led experts to warn of possible attacks on the multinational oil and gas assets in the region on at least two occasions in 2012. Despite those clear warnings, the composition of the plant's security force was not changed. The security forces at high-risk and high-value sites should be prepared to act quickly and effectively on the changing threat dynamics developed by predictive intelligence. Preparations should include objective analytics directly linked to the actionable procedures needed to improve measurable security enhancements. For example, accepting the In Amenas incident as a form of predictive intelligence, other sites should now:

    1. Reassess their relevant vulnerabilities and incorporate assault team attack response and mitigation measures in the site's emergency plans and exercise regimen;

    2. Enhance employee awareness of assault situational dynamics together with the reporting and response action protocols according to individual position and collateral position responsibilities; and

    3. Correlate situational awareness value and response expectations to other likely incident scenarios – for example, discovering an armed intruder on the site.

- *Reassess "Hardened" & "Remote" Target Analyses* – The remote geographic location of a critical infrastructure asset is often considered an attack deterrence. In the In Amenas incident, though, the remote location, combined with what seems to have been a lower local response capacity, may well have been viewed by the terrorists as an important operational advantage. Considering the planning, command, and control coordination necessary to seize such a large complex – and to wrest control from over 700 workers – the remote location gave the terrorists the critical time needed to subdue and dominate the site with little if any interference from external response forces. Positioning high-value and high-risk sites in remote locations may in fact result in greater vulnerabilities and greater reliance on internal and self-sustained capabilities.

- *Prepare and Practice for Extreme Scenarios* – Although the probability of multiple terrorist assault teams descending on a site seems to be remote, the adverse consequences to the site, its corporate assets, and the local community, coupled with broader cascading impacts, could be widespread. Therefore, developing, training, and exercising response procedures for such remote risks are prudent in preparing for more routine disruptive events. In that context, functional and capabilities-based preparations should include multidimensional threat scenarios including the relevant cascading complexities. Advance planning and the development of mandatory capabilities also should include the positioning of response elements beyond the site's property line – thereby integrating local and regional response assets of diverse emergency response disciplines into preparedness plans and activities. Vital response partners include off-site corporate assets and even multicorporate stakeholders having vested interests in the site.

  The In Amenas Gas Refinery did have a number of procedures in place to cope with a terrorist assault – including the actions assigned to workers in housing areas, other support sites, and the processing control rooms. The site procedures included alarm announcements and follow-on duty and responsibility assignments. Official reports show that the efforts of one security guard saved numerous lives by the prompt and effective actions he took in the opening moments of the attack – actions that cost him his own life. Only through practice and scenario-based exercises can site personnel perform in predictable ways when faced with real-world contingencies.

- *Prepare Responders for Special Site Hazards* – Counterterrorism and police response preparedness to sites containing particular internal hazards require specialized awareness, analysis, and skills unique to responder disciplines and properly aligned with their own individual and team capabilities. Unfortunately, the Algerian response forces at the In Amenas Gas Refinery lacked the preparatory experience needed to cope with the hazards posed by engaging in live-fire interdiction in the areas around pressurized flammable gas processing units at the site. It is still not known, in the open-source reports currently available, what plans the Algerian forces involved might have had in place for deploying T-72 battle tank main guns and/or firing helicopter gunship rockets in the final assault on the Tiguentourine processing facility. These heavy-gun assets do not seem to have been fired, but the question of consequence analysis as a part of any decisional criteria is relevant nonetheless.

  Site preparedness planning, careful coordination, and analysis of on-site hazards with law enforcement response teams are all of critical importance well in advance of an incident. Law enforcement response teams must prepare for alternative solutions and/or determine acceptable-risk thresholds for engaging live-fire, pyrotechnic diversionary, and other interdiction assets at or in areas containing special hazards such

AP4C

Handheld
CWA, TICs/TIMs
chemical detection
in confidence

Easy to use,
reliable, sensitive
and always ready

PROENGIN
Chemical and biological detection system

PROENGIN, inc.
140 S. University Dr, Suite F
Plantation, FL 33324 USA
Ph: 954.760.9990
contactusa@proengin.com
www.proenginusa.com

as volatile and flammable materials and/or toxic-release chemicals. Law enforcement should therefore assess such dangers and consider shifting to the use of frangible ("soft") ammunition for operations on certain sites. Such operational decisions should be predicated with analysis, training, and decisional procedures well in advance of active operations on relevant sites. The members of law enforcement interdiction units also should be prepared to operate effectively and to use the full ensemble of personal protective equipment needed to cope with the site's inherent hazards.

- *Compartmentalize the Site* – In addition to establishing security layers, concentric rings of ever-increasing monitoring and barriers to access include interior compartmentalization of critical assets and safe rooms for the staff in the area. Most modern chemical facilities compartmentalize their process control rooms with access controls. In many cases, though, very little is done to harden the access point and other areas within the facility by the use of simple doorstop wedges, shades over windows, robust locks and hinges, and interior solid-core doors. Using these relatively simple assets would significantly delay armed intruders from accessing areas and entering off-limits rooms as they search for potential victims to shoot or hostages to seize.

  At In Amenas, many workers used improvised hides such as under desks after locking and securing the doors. As terrorists searched the site, they attempted to kick in doors but, if the door withstood a few kicks, they moved on with their search. Despite possessing explosives that could have easily blown in locked unyielding doors, the terrorists chose to leave those rooms unchecked, which saved a number of potential hostages the fate of their less fortunate colleagues.

- *Strengthen Staff Self-Reliance & Critical-Incident Decision Making Capabilities* – Staff preparedness extends well beyond employees to include contractors and even visitors. Building preparedness also includes developing prudent self-reliance – to the point that staff skills and capabilities are sufficient for empowering critical incident decision making (commensurate, of course, with the positional duties and responsibilities of each employee). The analysis of numerous survivor reports suggests that most workers at the In Amenas Gas Refinery were in fact prepared to respond appropriately to an alarm and/or the receipt of information of a terrorist assault in ways appropriate to their locations and to their collective as well as individual positional duties and responsibilities. Even workers still in the Al-Hayat complex were well aware of the need to take the personal protective measures of hiding when faced with an assault on the site.

As mentioned earlier, security officials and process engineers seem to have performed their duties as best they could under the extremely difficult circumstances involved. Each worker's individual response efforts, adapted to the rapidly changing situational dynamics, posed an opportunity to save lives and at least mitigate other harmful consequences. After hiding for a full day, 45 workers escaped to safety because of the early warning provided by a security guard and their own adaptive ingenuity. Here, the lesson learned is that responsible and prudent staff empowerment can and should be an important preparatory measure that is likely to yield an exponentially greater return on investment in mitigation, to prevent undesirable consequences, and to greatly enhance a broad spectrum of recovery efforts as well.

Joseph Trindal is president and founder at Direct Action Resilience LLC, where he leads the company's portfolio of public and private sector preparedness and response consulting, training, and exercise services. He also serves as president of InfraGard National Capital Region Members Alliance. He retired in 2008 from the U.S. Department of Homeland Security, where he had served as director for the National Capital Region, Federal Protective Service, Immigration and Customs Enforcement. In that post, he was responsible for the physical security, law enforcement operations, emergency preparedness, and criminal investigations of almost 800 federal facilities throughout the District of Columbia, Northern Virginia, and suburban Maryland. He previously served, for 20 years, with the U.S. Marshals Service, attaining the position of chief deputy U.S. marshal and incident commander of an emergency response team. A veteran of the U.S. Marine Corps, he holds degrees in both police science and criminal justice.

Unique Dangers Posed by Lone-Wolf Terrorists

By Jeffrey D. Simon, Law Enforcement

So-called "lone-wolf" terrorists have proved time and again that they can initiate attacks that match and even surpass the death toll and destruction wrought by large, better known, and much better financed terrorist organizations. In Norway, for example, Anders Breivik set off a bomb in Oslo on 22 July 2011 that killed eight innocent people, then traveled to Norway's Utoya Island and massacred 69 more, many of them teenagers attending a political summer camp.

Meanwhile, in the United States, Major Nidal Malik Hasan, an Army psychiatrist, is accused of opening fire at Fort Hood, Texas, on 5 November 2009 – killing 13 people and wounding 32 others in the worst terrorist attack ever to take place on a U.S. domestic military installation. More than three years later, he is still awaiting trial (which is scheduled to begin this May).

Not quite eight years earlier, shortly after the 9/11 attacks, an anonymous attacker (believed by some to be a government microbiologist at Fort Detrick, Maryland, who later committed suicide) sent letters filled with anthrax spores to several Congressional offices and media news rooms, creating a new crisis atmosphere about the potential threat of a bioterrorism attack.

Creative, Empowered & Elusive Predators

Despite their usual anonymity and lack of "partners," lone-wolf terrorists share a number of typical characteristics – the first and perhaps most dangerous of which is that, because there is no group decisionmaking process involved that might stifle individual creativity, lone wolves are free to carry out any type of attack they might think of, with little or no fear of the likely consequences. This independence has led to some of the most innovative attacks in terrorism history. For example, lone wolves were responsible for the first U.S.:

- Vehicle bombing – a horse-drawn wagon filled with dynamite was detonated in New York City in 1920, killing more than 30 and injuring several hundred others;
- Major midair plane bombing – a bomb that was packed in a passenger's luggage exploded over Colorado in 1955, killing 44;
- Airplane hijacking – a National Airlines plane was hijacked and diverted from Florida to Cuba in 1961 (the crew and passengers were not harmed); and
- Anthrax letter attacks – mentioned earlier, killing five people and sickening 17 others.

A second "typical" characteristic about lone wolves is that they have little or no constraints limiting their level of violence. They are seldom if ever concerned about alienating supporters (as at least some terrorist groups might be), and they do not seem to fear a potential government crackdown following an attack. This latter trait makes them prime candidates to use weapons of mass destruction, specifically including biological or chemical agents, which usually are available on the open market.

A third generalization is that it is extremely difficult to identify and/or capture lone wolves. There are usually no communications to intercept and/or members of a group to arrest and interrogate about potential plots. This can be seen most obviously in the case of Theodore Kaczynski, the infamous "Unabomber" who was responsible for 16 bombings that killed three people and injured 23 more – but was able to elude law enforcement for almost 18 years (1978-1996). He was finally captured in early April of 1996 and is now serving a life sentence without parole.

A Carefully Planned Attack

Lone wolves can also be quite devious in planning a terrorist operation. A prime example is Eric Rudolph, an antiabortion lone wolf who set off a bomb at the 1996 Summer Olympic Games in Atlanta, Georgia, that killed one person and injured more than 100 others (a cameraman also died from a heart attack as he ran to cover the incident). He later bombed two abortion clinics, killing one person and, in an alleged attempt to kill homosexuals – a lesbian nightclub. At the scene of some of his attacks, he also planted second bombs that were set to explode after police and other emergency responders had

arrived to deal with the initial explosions. In one case, police discovered the second bomb and defused it, but in another case the second bomb went off as planned, injuring several people, including police officers. Rudolph was finally arrested in 2003 and is now serving a life sentence without parole.

Breivik, the Norwegian anti-Islamic lone-wolf terrorist, apparently set off the bomb in Oslo primarily to divert the attention of law enforcement personnel so he could then travel to Utoya and kill as many as possible of the young people attending the summer camp there. He wore a policeman's uniform and told camp officials – who had already heard the news about the Oslo bombing – that he was there to protect the campers. Breivik then walked to the area where the campers' tents were located and began shooting as many people as he could find.

Following the Norway shootings, one police official stated that Breivik "just came out of nowhere." Another claimed that there had been "no warning lights" that Breivik was a terrorist. Their statements seem to imply that there is little if anything that can be done to prevent lone-wolf terrorist attacks. That is not quite the case, though. On the contrary, Breivik had actually made his presence known by using the Internet to purchase large quantities of ammonium nitrate fertilizer – which he later used to build the car bomb that he set off in Oslo. Norwegian authorities were initially suspicious of Breivik's online purchase, but erroneously concluded that the fertilizer was in fact intended for agricultural use on a farm that Breivik had rented.

Breivik also advocated violence a number of times in a 1,500-page "manifesto" that he posted online shortly before his murderous attacks. "Once you decide to strike," he wrote, "it is better to kill too many than not enough, or you risk reducing the desired ideological impact of the strike." Like many other lone wolves, Breivik therefore did not, as suggested, simply "come out of nowhere."

Preventive Strategies

Through a mix of creative and innovative strategies, it is in fact possible to reduce the likelihood of a lone wolf succeeding in an attack. Such strategies include: (a) improving detection devices in post offices and other facilities to help identify, in advance, package bombs or letters containing anthrax spores; (b) expanding the number and use of closed circuit television (CCTV) cameras in public buildings and other settings; (c) accelerating the further development of computer technology that can recognize "suspicious" behavior in public places – and instantly forward the information to a control center where the decision whether or not to notify the police would be made; (d) further advances in biometrics, including the use of gait analysis to determine the speed, stride, and other characteristics of a person's walk to determine if that person may be carrying a bomb or other weapon; and (e) the analysis of facial expressions to predict hostile intent (an obviously difficult task).

The crimes of lone-wolf terrorists are difficult, but not always impossible, to prevent. New strategies are being used to reduce such threats within the United States.

Another potentially important strategy for identifying lone wolves before they strike is to monitor the Internet – but without violating the civil liberties of law-abiding citizens – to identify those who are visiting extremist chat rooms, purchasing bomb-making materials and/or other suspicious items online, or posting ominous threats and manifestos.

In short, the lone-wolf threat seems likely to grow in the coming years. The current age of terrorism is one in which any number of people can become knowledgeable, empowered, and radicalized via the Internet and other means. Today there is also the possibility that at least some of the insurgents from the wars in Iraq and Afghanistan might later take their expertise to other regions and launch individual attacks. It is therefore important that governments and societies be as committed to dealing with the lone-wolf terrorist threat as they have been to the threat posed by al-Qaida and other terrorist groups.

Jeffrey D. Simon is an internationally recognized author, lecturer, and consultant on terrorism and political violence. He is president of Political Risk Assessment Company Inc., and a visiting lecturer in the Department of Political Science at UCLA. His most recent book, Lone Wolf Terrorism: Understanding the Growing Threat*, was published in 2013. A former RAND analyst, he has conducted research and analysis on terrorism for more than 25 years. His writings on terrorism, political violence, and political risk have appeared in many publications, including the Journal of the American Medical Association, Foreign Policy, and the New York Times. His website can be found at* http://www.futureterrorism.com*. He earned a B.A. in History from the University of California at Berkeley, an M.A. in Political Science from Indiana University, and a Ph.D. in Political Science from the University of Southern California.*

Safer Schools Through Advance Planning

By Donald J. Cymrot, with Stephen E. Rickman, Viewpoint

In response to the 14 December 2012 school shootings in Newtown, Connecticut, President Barack Obama has offered a wide range of executive orders and proposals – including several specifically intended to make schools safer. One major component of his safe-schools proposal is to ensure that *all* of the nation's schools have effective and comprehensive emergency management plans in place. As part of that proposal, he charged the federal government's Departments of Education, Justice, Homeland Security, and Health and Human Services with developing a model set of emergency management plans.

These model plans will presumably supplement earlier guidelines published in 2006 by the Readiness and Emergency Management for Schools Technical Assistance Center of the U.S. Department of Education. The previous guidelines provide what seems to be a reasonably broad framework for such plans, but a recent review by CNA of emergency management plans for school districts in the greater Washington, D.C., area found them lacking the specific details needed to make them operationally effective.

To begin with, each school in the nation has unique security considerations. However, because security plans are often developed at the district level, they are usually not customized enough for each and every location in the district. For example, response time is a critical factor in emergency planning. Schools built at a greater distance from hospitals or police stations have needs, therefore, that might be considerably different from those of schools located closer to such emergency facilities. Moreover, sprawling one-story schools with many exits may well have security needs considerably different from those of other schools – two or more stories high, perhaps, and with only a few exits. District-level plans often do not recognize or account for such differences.

To ensure the safety of the nation's schools – and the children, teachers, and others inside the school – administrators and planners must assess the unique characteristics of each school and adjust their emergency management plans accordingly.

Deterrence First, Plus Improved Communications

A truly comprehensive plan also would include sections not only on response and recovery but also – to deter or avoid incidents – on prevention, protection, and mitigation. That same more detailed plan would probably also include the establishment of a clear chain of communications to report threatening statements, suspicious behavior, and/or any other evidence suggesting a possible intent to commit mass violence on school grounds.

Also included in the more comprehensive plan would be designation of the school officials specifically responsible for screening – and, if necessary, relaying – information to law enforcement and healthcare agencies; also, in a worst-case scenario, to the families of students and members of the school's staff. Armed with such information, first responders and local officials would then be able to work effectively with school staffs to develop the detailed guidance needed for reporting and responding to potentially dangerous incidents.

Some current plans do not cover scenarios specific to mass shootings, which should at least provide: (a) the information that should be relayed in 911 calls (e.g., location of shooter, the type of weapon used); (b) the varying factors that must be considered when deciding whether to shelter in place, lock down, or evacuate; and/or (c) a list of the school officials authorized to make such decisions. Moreover, some plans do not even spell out in detail the communications and coordination also required – between school officials and first responders – to cope with such incidents.

Drills & Exercises: What, When & How Often?

Many plans now in place also lack even a modest list of training and exercise requirements. More effective plans

would specify not only who should participate in such training but also how, and how often, the entire school should conduct a drill or exercise. Of particular importance in this area would be the need to conduct joint exercises with first-responder agencies. Schools that carry out emergency response drills following the same scenario each and every time miss the opportunity to identify gaps and shortfalls in the response to different types of emergencies because repetition of the same drills becomes mechanical in execution. The use of varying scenarios would allow officials to review the results and modify the plans as needed.

The federal government will likely post the model plans online. But those plans would not, by themselves, make schools safer unless school officials, working in conjunction with first responders, tailor the model plans to local circumstances. In his comments to the nation following the Newtown shootings, President Obama acknowledged that the vast majority of the nation's schools already have emergency management plans on paper, but barely half of the schools had exercised those plans in recent years. That responsibility falls on local school officials and first responders.

By reexamining existing emergency management plans, local officials can help to ensure that the plans being revised, promulgated, and implemented provide enough detail and flexibility to support decision-making in rapidly unfolding events. Planning to cope with mass shootings is a particularly difficult challenge because such shootings tend to be extremely rare events. In a year or two, as new issues arise, vigilance may fade, but local officials must overcome the complacency of quietude. If they do not, U.S. schools will continue to be vulnerable, and the nation may face the terrifying prospect of another Newtown tragedy in the not-too-distant future.

Donald J. Cymrot is a vice president at CNA, a not-for-profit research and analysis organization. He directs both the quality management system in one of CNA's operating units and the education practice. He leads CNA Education in conducting research and providing technical assistance on a variety of topics from pre-kindergarten to post-secondary and workforce issues. Among his recent efforts is an initiative to improve emergency planning within schools. Previously, he directed CNA's manpower and training research team for which he was awarded a Superior Public Service Medal by the Department of the Navy. He holds a Ph.D. in Economics from Brown University.

Stephen E. Rickman is the director of Justice Programs at CNA. Previously, he was the director of the D.C. Emergency Management Agency and director of readiness for the White House Office of Homeland Security.

Staying Ahead of "The Big One"

By Joseph Cahill, EMS

When the average citizen is confronted by an emergency situation beyond the routine, he or she is usually overwhelmed and forced to rely on emergency responders to take command and re-establish control. Unfortunately, the first responders themselves do not always have the same option. Their first task, usually, is to restore some degree of order over the situation – but they must first impose an even higher degree of order on themselves. For that reason alone, when sudden disasters reach such magnitude not only are the average citizens on the scene overwhelmed, but also the internal resolve of professional responders (and response agencies) need all of the tools required to carry out their work.

To meet that daunting challenge, the leaders of first-responder agencies must plan, equip, and practice for major events in such a way that the responder personnel are less likely to be overwhelmed – and, of even greater importance, can continue to function at a high level of efficiency.

The advance planning required starts, of course, with routine day-to-day operations and expands into the specialized field of disaster management. Whatever the situation, all plans should be based on what is usually the same and very specific set of goals: restore order and save lives. With the correct organizational structure in place, planners can expand a supposedly "typical" day-to-day plan to meet and deal effectively with rapidly escalating situations. More importantly, when responders understand both the goal and the guidelines, they can use and quickly expand upon the same plan when an incident escalates to the "overwhelming" point mentioned earlier. That type of plan, and the attitude it fosters, allows responders to focus on goals already familiar to them rather than try to remember the specifics of several different plans.

Quantity as Well as Quality: Both Are Needed

In much the same way, and for the same reasons, the purchase, transport, and use of the equipment needed to cope with a major incident is often a matter of expanding

the quantity and/or amount of day-to-day equipment used by and familiar to the individual responder and responder teams. In situations where the number of casualties is unknown (but might be above what is considered to be the local "norm"), transporting the supplies required to treat several patients, rather than what is needed to treat only one or two, is the most useful contingency plan to follow at the unit level.

There are several other steps, though, that can be taken at the macro-level – for example, special vehicles or trailers big and powerful enough to carry large quantities of supplies and equipment can be purchased and strategically located to be accessible when needed. Similarly, the purchase and deployment of mass-treatment "units" – i.e., vehicles large enough to treat multiple patients and/or even tent facilities that can be set up on-site – is a common strategy used for treating several patients either simultaneously or immediately following a high-casualty incident or event.

Also at the command level, the tools needed to maintain organizational continuity and efficiency, typically through an Incident Command System (ICS) model, can be invaluable in carrying out critical management-type functions such as tracking not only the number and qualifications of the responders on-site but also the destination of patients who have been removed from the incident scene (to hospitals or other healthcare facilities). These same "tools" often take the form of magnetic boards or laptops fitted with specially designed emergency-management software. Additionally, the use of such visual cues as helmets, or brightly colored vests and easily read identifiable markings (signifying the varying roles of individual responders), is helpful in maintaining control over an event.

Chaos & Common Sense; Clarity & Coherence

ICS is not only the law of the land but also an effective operational strategy for maintaining control over: (a) a chaotic scene; and (b) the arrival and use of multiple units from many agencies. Unfortunately, like many other elements of disaster plans, the use of an advanced-capability ICS frequently is ordered only when "the big one" – a tornado, earthquake, or terrorist attack, for example – occurs. This is as much a mistake as any other type of disaster planning process that deviates significantly from the usual day-to-day operational tempo.

Common sense usually prevails, fortunately. If an agency's plans are designed to build on the day-to-day operations that are the usual norm, staff usually can stay ahead, mentally, of any task assigned by considering, in advance, how to expand the operational response needed if and when the incident itself expands in scope and/or severity. In other words, this thought process itself has to become the operational norm.

Following a coherent line starting with a statement of goals – then through planning, equipping, and consistent implementation during daily operations – will help prepare staff not only for the expected situations but also for larger incidents when circumstances may be described as "overwhelming."

Joseph Cahill is a medicolegal investigator for the Massachusetts Office of the Chief Medical Examiner. He previously served as exercise and training coordinator for the Massachusetts Department of Public Health and as emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as citywide advanced life support (ALS) coordinator for the FDNY – Bureau of EMS. Prior to that, he was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem. He also served on the faculty of the Westchester County Community College's Paramedic Program and has been a frequent guest lecturer for the U.S. Secret Service, the FDNY EMS Academy, and Montefiore Hospital.

Phoenix

Lightweight, low burden CBRN protection

Phoenix

Lightweight CBRN protection suit

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

http://frontline.remploy.co.uk

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

Remploy
Putting ability first

Frontline

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

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

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

U.S.-Mexico Border Security – The Spillover Effect

By Richard Schoeberl, Law Enforcement

Over the past several years, the United States has experienced increasing levels of crime related to drug trafficking – and, more specifically, to drug-related homicides along the 2,000-mile stretch of border between the United States and Mexico. Violent incidents on the U.S. side of the border that have been attributed to Mexico's criminal gangs and cartels suggest that an escalation of "spillover violence" in that region may well be on the rise. Moreover, according to the BBC, as many as 70,000 people in Mexico have died in drug-related violence, and more than 26,000 have been reported as missing, since Mexico's then-President Felipe Calderón declared war on drug cartels in 2006.

Crime Reports – Statistics & Limitations

Based on data compiled by the Trans-Border Institute at the University of San Diego, homicides related to organized crime increased by almost 700 percent from 2007 (822) through 2012 (5,623) in the period between January and November in the six Mexican states that share the border with the United States – Baja California, Sonora, Chihuahua, Coahuila, Nuevo Leon, and Tamaulipas. This concentration of crime along the border can be attributed in large part to the fact that the United States remains the largest consumer of the multi-billion dollar market of illegal drugs.

An unsettling report released to Congress in February 2013 by the Government Accountability Office (GAO) speculated that the seemingly endless drug war in Mexico will continue to escalate and ultimately cross the southwest border into the United States itself. The same report indicated that federal law enforcement agencies lack the advanced technology needed to track what might be considered "spillover" crime.

It is both unrealistic and ingenuous to assume that Mexican crime/drug cartels leave their weapons, violence, and criminal intentions at the border check point before entering the United States.

Currently, according to the GAO, the only means of measuring spillover violence comes from the Federal Bureau of Investigation's (FBI) Uniform Crime Reporting (UCR) Program, which provides a standardized method to track crime levels in border counties. However, the UCR data is somewhat limited because it: (a) Simply provides a national view of crime that is based solely on the "voluntary" submission of a variety of statistics by city, county, and state law enforcement agencies; and, more importantly, (b) lacks the ability to link crimes associated with spillover crimes from Mexico – for example, cartel or organized crimes related to drug trafficking.

The UCR data, therefore, cannot be used or relied upon solely to determine to what extent crimes can reasonably be attributable to spillover from Mexico. The rationale here is that the UCR Program does not collect similar data on all types of crimes committed in the United States that have been associated with Mexican drug-trafficking organizations – particular types of kidnappings and/or home invasions, for example. Another understandable problem is that people who have been attacked or robbed in the course of unlawful activities may be reluctant – for fear of retaliation, deportation, or both – to report their own involvement to law enforcement. For that reason alone, many crimes connected to drug trafficking go unreported. When both the victim and the offender are in the United States illegally, that relevant information will seldom if ever show up on the UCR.

Defining "Spillover"

The "legalese" used presents yet another problem. Without a legal definition for "spillover violence," it is difficult for many government agencies to track and analyze such statistics. As stated in Congressional testimony on 5 May 2010 at the U.S. Senate Caucus on International Narcotics Control, "Spillover violence entails deliberate, planned attacks by the cartels on U.S. assets, including civilian, military, or

law enforcement officials, innocent U.S. citizens, or physical institutions such as government buildings, consulates, or businesses." However, the testimony continued, "This definition does not include trafficker-on-trafficker violence, whether perpetrated in Mexico or the U.S."

According to a 28 February 2013 Congressional Research Service Report, "There is no comprehensive, publicly available data that can definitively answer the question of whether there has been a significant spillover of drug trafficking related violence into the United States. Although anecdotal reports have been mixed, U.S. government officials maintain that there has not yet been a significant spillover."

Not all members of Congress accept the administration's position. Even so, it seems obvious that the key to determining whether spillover violence is occurring at the same rate, on the rise, or subsiding starts with accurately defining the term "spillover." The difficulty facing the executive branch of government, therefore, is not only in determining how and when to define the problem, but also how to statistically track and classify the term spillover violence – all of which must be done before an acceptable resolution can be applied to the problem.

Conflicting Views From Up Close & Far Away

Many members of Congress, as well as law enforcement officials from state and local agencies along the nation's southwest border, have long argued that drug-linked crimes are in fact "spilling" over the border from Mexico. Moreover, a 2011 Gallup/USA Today poll indicated that, at that time, 83 percent of Americans believe the rates of violence are in fact higher along the U.S. southwest border than they are anywhere else in the United States. Although U.S. federal law currently does not require gathering facts on spillover crime, two new bills – H.R. 2124 and H.R. 6368 – have been introduced in Congress in an attempt to require federal agencies to report all occurrences of cross-border violence.

Obama administration officials have frequently claimed that, thanks to a substantial upsurge in the

federal law enforcement presence along the southwest border, crime rates have plummeted dramatically – and the U.S.-Mexico border is safer now than it had been in the past decade or so. White House officials base that putative decrease on the FBI's UCR program. The UCR, though, includes data only on such crimes as murder, rape, robbery, and aggravated assault, but does *not* keep track of many of the crimes committed by drug traffickers – specifically including kidnapping, extortion, public corruption, drug and human smuggling, and trespassing.

Although the Obama administration claims that the southwest border is now "statistically" safer than before, officials in the bordering states have long warned of an invasion of Mexican cartels and gangs. In September 2011, retired U.S. Army General Barry McCaffrey and Major General Robert Scales contributed to a report, along with the Texas Department of Public Safety (which co-sponsored the report – with the Texas Department of Public Safety) cautioning that there has been an increase of violence along the southwest border region, specifically Texas, and suggesting that the Texas side of the border has now become a "combat zone."

The same report described how Mexican cartels are demonstrating a clear intent to "move their operations into the United States" – and McCaffrey personally asserted that, "During the past two years, the southwestern United States has become increasingly threatened by

the spread of Latin American and Mexican cartel organized crime."

Assessing the Real Threat

The 2011 threat assessment carried out by the U.S. Department of Justice's National Drug Intelligence Center indicates that: (a) The Mexican transnational criminal organizations now pose the greatest drug trafficking threat to the United States; and (b) The demand for illicit drugs in the United States partially drives this threat. Obviously, establishing a realistic timeline for measuring the fluctuations in drug trafficking-related violence over the past decade or so could be of vital importance in determining what must be done next.

Whatever else happens, though, there definitely is a major disagreement about the definition and classification of "spillover violence" and the extent of such violence. Nevertheless, there is still concern about what will happen if the current resources needed – manpower and funds – to combat the threats faced at the border are further restricted. The U.S. Customs and Border Protection (CBP) is just one agency being forced to reduce its operating budget as part of the ongoing "sequester." Following, from a statement released by the CBP earlier this month, is how that agency views the possible new cuts that might be required:

> "In order to address the more than half a billion in budget cuts imposed by sequestration, U.S. Customs and Border Protection must take significant budget reduction actions. CBP will continue to make every effort to minimize the sequester's impact on public safety and national security, but expects that planned furlough of employees, along with reductions to overtime and hiring freeze will increase wait times at ports of entry, including international arrivals at airports, and reduce staffing between land ports of entry. Even with these cuts, though, individuals apprehended illegally crossing the southwest border will still be processed as usual. CBP continues to evaluate further impacts of sequestration on our operations. Because the length of the sequestration as well as funding levels through the end of the fiscal year are unknown at this time, it is difficult to project the impact of the reductions on individual employees or job occupations."

Current & Future Concerns

Unfortunately, the CBP faces cuts of $595 million in 2013 under the automatic cuts previously projected to go into effect later this month. On 21 March, Congress passed a stop-gap resolution that postpones most of the sequester cutbacks until 30 September 2013. Nonetheless, the budget cuts projected earlier still include a reduction in border patrol agents and a cut in the funding allocated for the so-called "virtual fence" along the U.S.-Mexico border.

Obviously, the leadership at the U.S. Department of Homeland Security is still very concerned about the effect of the cutbacks projected earlier. "I don't think we can maintain the same level of security. … If you have 5,000 fewer Border Patrol agents, you have 5,000 fewer Border Patrol agents," Homeland Security Secretary Janet Napolitano said in a *Washington Times* interview on 25 February 2013. The United States has already allocated significant resources to securing the U.S.-Mexico border, but the reductions still projected will undoubtedly create new concerns over whether, and how, southwest border violence and drug trafficking can be contained.

Clearly, the level of "spillover violence" into the United States as a result of the Mexican drug war is determined by: (a) The statistics that are used; (b) how the data gathered are interpreted; and, most significantly, (c) where someone lives – in Washington, D.C., or somewhere along the southwestern U.S. border. Despite reports issued in Washington, D.C., indicating that the southwest border is statistically safer now than in the recent past, many local residents as well as state and local law enforcement officials along the U.S.-Mexico border would strongly disagree.

Richard Schoeberl has more than 17 years of counterintelligence, counterterrorism, and security management experience, most of it developed during his career with the Federal Bureau of Investigation, where his duties ranged from service as a field agent to leadership responsibilities in executive positions both at FBI Headquarters and at the U.S. National Counterterrorism Center. During most of his FBI career he served in the Bureau's Counterterrorism Division, providing oversight to the agency's international counterterrorism effort. He also was assigned numerous collateral duties during his FBI tour – serving, for example, as a Certified Instructor and as a member of the agency's SWAT program. He also has extensive lecture experience worldwide and is currently a terrorism and law-enforcement media contributor to Fox News, Sky News, al-Jazeera Television, and al-Arabiya.

Missing in Action: Private-Sector Situational Awareness

By Michael J. Pitts, Private Sector

Most adult Americans can personally recall the terrorist attacks against the United States on the morning of 11 September 2001, but many may already have forgotten what happened on the morning of 19 April 1995. Among the questions that can be posed about private citizens are the following: (a) What was the situational awareness of the persons directly affected by those two national tragedies before disaster struck (at about 9:00 a.m. locally on both of those dates)? (b) How aware is the average U.S. citizen and/or local resident of the events and situations – anywhere, and on any date – unfolding around him or her? (c) More specifically, what is their "fight or flight" reaction to manmade versus natural disasters?

Although many Americans may vaguely recall the name Timothy McVeigh, they typically may not remember that in April 1995 he was the person who rented a truck, loaded it with chemical explosives, and used it to destroy the Alfred P. Murrah Federal Building in Oklahoma City – killing 168 adults and children, injuring hundreds of other persons, and damaging several nearby buildings.

The morning of 11 September 2001 – a date that certainly should be remembered by most American adults alive on that day – started when 19 men linked to the al-Qaida terrorist group hijacked four commercial airliners and flew them, laden with jet fuel and filled with innocent passengers, into the Twin Towers in New York City, the Pentagon in Washington, D.C., and a remote field of grass in Shanksville, Pennsylvania.

Those deliberate, carefully orchestrated, and almost simultaneous acts of terrorism killed nearly 3,000 civilians, military personnel, and first responders. They also injured thousands of other people, and destroyed several other buildings in the area close to the Twin Towers. The violence of the 9/11 attacks not only changed the lives of those who died or were seriously injured – and the lives of their families, friends, and relatives – but also changed the nation as a whole.

Identifying the Warning Signs

In general, situational awareness involves being alert to what is happening in the immediate vicinity of the individual citizen and, through that awareness, understanding how information, events, and personal actions can directly affect his or her surroundings, both immediately and in the future. Having little or no situational awareness is often a primary factor in incidents attributed to human error.

Situational awareness is particularly important in disciplines where: (a) the information flow is relatively high; and/or (b) poor decisions can lead to serious consequences – for example, when the person making the decision is functioning as a soldier, piloting an aircraft, or treating critically ill or injured patients. Despite those obvious examples, developing and maintaining situational awareness also can be a critical and even life-saving skill for citizens traveling within and between cities, working in an office building, or simply remaining inside their homes.

Seen in that light, the attack on the Alfred P. Murrah Federal Building was a clear warning for the nation's public and private sectors alike – largely because that criminal act was planned and carried out not by a foreign-born and ideologically motivated terrorist but by a former U.S. soldier and three other American accomplices. Unfortunately, several other multi-victim attacks occurred on U.S. soil that specifically targeted school children (of all ages): Columbine High School in Colorado (20 April 1999); the Virginia Polytechnic Institute and State University (16 April 2007); and, most recently, the Sandy Hook Elementary School in Newtown, Connecticut (14 December 2012).

The faculties and staff at all of those schools undoubtedly had at least some vaguely worded type of plan in place to avoid and/or at least mitigate potential acts of violence, but obviously much more can and should be done. Thus, with an increase in violent shootings and a decrease in available funds, the private sector can play a valuable role in increasing the collective situational awareness in their own communities.

Understanding the Phases of Emergency Management

Improving the overall situational awareness of small businesses, non-profit organizations, major corporations, and individual citizens necessarily requires, among other things, large but carefully managed investments of time and money as well as additional resources in emergency management – people as well as equipment. It also involves

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

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

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

FLIR®

www.FLIR.com/gs

upgrading the processes and mindsets needed to protect both the local population and the community's critical assets from numerous hazards and risks caused by manmade disasters – including active "lone wolf" shooter incidents – and/or natural catastrophes. And, in responding to any of these events and incidents, it involves steps that management and individual citizens must take to ensure the resiliency of the organization, office building, or prvate home. To do all this, though, starts with an understanding of the four distinct phases of emergency management: mitigation, preparedness, response, and recovery.

Mitigation can perhaps best be described as the effort needed to reduce the loss of life and property by lessening the impact of disasters. It is defined more specifically, on the website of the Federal Emergency Management Agency (FEMA), as "taking action before the next disaster to reduce future human and financial consequences." Effective mitigation processes and actions also require a clear understanding of local risks, the need to address – and actually make – a number of difficult choices, and a willingness to invest the resources needed to help ensure the community's long-term well-being. Without taking these and other mitigation actions, local businesses and the community at large have only one alternative: accepting the fact that there may well be greater safety, financial security, and self-reliance risks in the future. Personal mitigation, on the other hand, is mainly about knowing and avoiding unnecessary risks, which includes an assessment of the possible risks – to individual/family health and/or to private property – posed by an active shooter or by acts of nature.

Preparedness refers to actions taken as precautionary measures in the face of potential disasters. These actions include physical preparations such as: modifying buildings to survive earthquakes and floods; stockpiling emergency supplies; planning and publicizing local evacuation routes; and training groups, organizations, and individual citizens for emergency action. Preparedness is a critical step in recognizing and mitigating negative outcomes from incidents such as an active shooting or a terrorist bombing and includes coordination with public health agencies and local emergency responders.

Response usually begins with search and rescue operations, but the focus can quickly turn to fulfilling the basic humanitarian needs of the affected population. The effective public-private coordination of disaster assistance also is crucial, particularly when many organizations respond and the demand caused by the disaster exceeds the capacity of local emergency responders.

Recovery, of course, almost always starts after the immediate threat to human life apparently has ended – and continues until such time as: (a) the local infrastructure has been replaced or repaired; (b) electric power, water, and other functional needs have been restored; and (c) everyday life is back to normal (however that sometimes vague word is described).

The FEMA Reading File: For Personal & Collective Safety

Fortunately, there are many helpful FEMA courses already available on the development and improvement of situational awareness for businesses, groups, and individual citizens. Included in the agency's forward-looking curriculum are instructions, for example, in situational awareness, workplace violence, facility security, home and small business protection, and school safety.

Other courses also are available on such topics as public-private partnerships, emergency preparedness, natural and manmade disasters, individual citizen and community preparedness, and the dangers posed by hazardous materials. Community organizations and businesses would be well advised to at least investigate the value of these courses in developing and sustaining peer-support and critical-incident response teams.

Ultimately, situational awareness begins with developing increased vigilance on the part of the individual citizen – adults, teenagers, and even younger children. When businesses increase and improve local/community situational awareness by educating and training their own employees on the specifics of emergency preparedness and disaster response, the private sector itself becomes more resilient and better able to prepare for, respond to, and recover from incidents with less reliance on first responders, FEMA, and/or other federal, state, and local agencies and organizations.

Michael J. Pitts is the managing director for the Readiness Action Division of Dr. Tania Glenn and Associates, PA (TGA), headquartered in Austin, Texas. Before joining TGA in 2011, he spent 30 years in federal law enforcement and government aviation: the U.S. Air Force and U.S. Army as well as the U.S. Immigration and Customs Enforcement and U.S. Customs and Border Protection. He is certified in critical incident stress management through the International Critical Incident Stress Foundation. He earned an Associate of Arts degree in military studies from the New Mexico Military Institute, a Bachelor of Arts degree in political science and international affairs from the University of Colorado, and master's degrees in public administration from Shippensburg University and in strategic studies from the U.S. Army War College.

Predictive Policing: Actionable Information About Potential Crimes

By Rodrigo (Roddy) Moscoso, Law Enforcement

The mainstream advertising of new capabilities for public safety data analysis may be leading to a smarter new world where police officers can arrive at the precise location of crimes before those crimes are committed. IBM's current television spot for the company's Software Package for Statistical Analysis (SPSS) shows a police officer "hanging out" at a convenience store (presumably sent there based on a prediction made by the SPSS system); when the prospective thief arrives, he sees the officer and promptly leaves the scene – crime averted.

The multiple benefits of such a capability are immediately obvious: Reduced crime, decreases in both violence and personal injuries, and lower insurance rates are just a few of the most obvious examples.

In addition, this next level of "smart" policing may enable law enforcement to truly do more with less by targeting enforcement in areas where crimes are the most likely to be committed. Today, in an environment of continuing fiscal austerity, new budget reductions may be inevitable. For that reason alone, a police force that is better informed by using analytics may be the most effective way to maintain a high level of public safety.

CompStat & Command Central

IBM's offering represents one of several predictive-analytics solutions that have entered the public-sector marketplace over the past decade. Building on the traditional "CompStat" (computer statistics) geospatial analysis/"heat" maps, these new solutions add value by analyzing traditional factors – including but not limited to the time of day, the day of the week, weather conditions, and modus operandi. Such solutions are now possible because of the huge growth of structured and unstructured data already compiled from new cross-jurisdictional datasets. The resulting analysis then can help identify the precise location of *anticipated* crimes – and can do so in near-real time – thereby providing a potential wealth of future tactical benefits.

In Caroline County, Maryland, for example, Captain James Henning used CrimeReports.com's "Command Central" analytical tools to map a series of burglaries that had taken place over a three-month period. After that information had been mapped, then grouped in accordance with the modus operandi of the crimes themselves, Captain Henning applied a spatial-analysis algorithm – developed from the CrimeReports toolkit – that correlated the days, times, and locations of the burglaries that had already occurred.

Henning then was able to create a progression map of where the perpetrators were most likely to commit a crime during the next several weeks and months. By overlaying the spatial and time predictions on a map of his local police patrol routes, Henning was able to focus his department's resources on specific areas and at specific times. "The rest was good old-fashioned police work," he commented. Armed with the predictive analysis, the task force conducting the investigation identified the most likely suspects in those areas. Eventually, by using traditional physical and electronic surveillance of the most likely suspects as the case progressed, they were able to make several arrests.

Countering Crimes in Real Time

The next challenge in the use of predictive analytics may be to engage law enforcement officers in the field, in real time, by identifying the most likely criminal activity through an *automated* alert system. Instead of relying on the traditional analysis of investigators reviewing data from various spatial-analysis tools, a "smart prediction system" could automatically alert officers already in the field by using specific locational information based on the real-time processing and analysis of the large volume of data constantly being ingested from multiple sources. Such a system could also be used to receive and analyze data in advance – received, for example, from incident reports, corrections and booking files, license-plate readers, suspicious activity reports, and electronic citations.

Coupled with other related factors – including date, time, and even weather conditions – the system could send a geographically defined alert to officers in a specific area (even across police jurisdictions) warning them that a particular type of crime may be likely to occur in a specific location. In addition, an officer conducting a routine traffic stop could receive a "predictive hit" based on the electronic submission of the driver's name and/or vehicle tag.

A smart analytical system also may identify the person or vehicle as a possible "triggering event" for such an alert – again, based on the time of day and day of the week, the specific location, weather conditions, and similar data – and use it to inform the officer on-scene that the person stopped and/or the vehicle may be associated with a particular crime – either current or *future*. The alert may then lead the officer to look for additional "clues" that the person or vehicle may be engaged in some type of criminal activity.

One example of how this situation could develop: An officer might be alerted to the fact that the vehicle or person fits a particular modus operandi for the theft of copper wire. Using that data and/or other information – e.g., equipment usually associated with commercial power maintenance – the officer then might look into the trunk and/or backseat of the same car or truck.

The Bright Future of "Predictive Hits"

Although various technical solutions now exist that already can be used to trigger an automated alerting capability, many important procedural issues also must be addressed before such systems become routinely used in a tactical environment. Most importantly, the notion of "probable cause" may take on a more literal meaning if an officer were to receive a "predictive" alert.

Two key questions that might be asked are the following: (a) What actions, if any, would an officer be allowed to take based on this type of alert? (b) If hearsay from a reliable source can serve as a probable cause, would a so-called "smart" analytical system alert be considered reliable enough for an officer to take preventive action?

It may be quite some time before these and other issues are fully considered and subjected to legal scrutiny. In the meantime, new technologies will continue to be developed and police departments will almost certainly feel the operational effects caused by smaller budgets and reduced work forces. The predictive policing-enabled mobile officer therefore may be the best alternative to ensure that the American people continue to be protected from current and future crimes.

Rodrigo (Roddy) Moscoso currently serves as executive director of the Capital Wireless Information Net (CapWIN) Program at the University of Maryland, which provides software and mission-critical data access services to first responders across dozens of jurisdictions, disciplines, and levels of government. Formerly with IBM Business Consulting Services, he has more than 20 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.

Police Training For Hazardous Threats

By Shannon Arledge, Exercises

Five police officers from Long Beach, California, recently trained at the FEMA (Federal Emergency Management Agency) Center for Domestic Preparedness (CDP) in Anniston, Alabama. The officers had enrolled in three courses to increase their own knowledge about toxic-agent or biological incidents. The training they received will in fact: (a) help all members of the Long Beach Police Department (LBPD) stay current with California safety mandates; and (b) lay the foundation for other low/no-cost training opportunities in the future.

"We have 800 officers in our department that require this type of training," said Sgt. Ryan Lebaron, LBPD training coordinator. "Attending these CDP courses provides us a credible background to deliver training at home following the Train-the-Trainer course we plan to take next."

Two of the three CDP courses the LBPD officers attended – the Law Enforcement Protective Measures (LEPM) and Law Enforcement Response Actions (LERA) – are intensive one-day sessions focused on

Five police officers from the LBPD respond to a potentially lethal hazmat incident at a mock courtroom, inside a simulated federal building.

law-enforcement response capabilities. Both courses provide detailed "hands-on" training on topics directly related to situations involving weapons of mass destruction – terrorist tactics and targeting, for example – with special focus on the response skills needed to cope with various CBRNE (chemical, biological, radiological, nuclear, and/or explosive) hazards and incidents. The final course of the very busy week was an eight-hour class simply called HOT (Hands-On Training) for CBRNE Incidents.

"This training provides a great deal of knowledge to safely respond to a hazardous incident," Lebaron commented. "It also provides refresher skills to properly manage a contaminated crime scene and … [to develop the] abilities to triage and decontaminate survivors if needed. When we are able to provide training at home, it will be beneficial for all of our officers, and the public we serve."

When the next toxic agent or biological incident occurs, graduates of FEMA's Center for Domestic Preparedness are better prepared to take the steps needed to protect the citizens in their home communities.

HOT Experience & A Win-Win Scenario

The HOT course requires participation in a day of training at the CDP's toxic-agent "practice field" – known as the COBRA (Chemical, Ordnance, Biological, and Radiological) training facility, which offers the only program in the entire country featuring emergency response training exercises using "real-life" toxic chemical agents and biological materials. The COBRA experience significantly enhances the ability of CDP graduates to effectively prevent, respond to, and recover from incidents involving chemical weapons and other hazardous materials.

"The confidence we gained in our equipment is a major take-away," said Lebaron. "It is one thing to be told how we should perform certain procedures, but until you get the first-hand experience … [working with actual toxic chemicals] you are not fully confident. Taking this knowledge home is a win-win for our department."

The end-goal for the LBPD is to both sustain and build on the skills, response actions, and protective measures learned during the CDP training. The attendees then will be expected to provide the same type of training locally, at the basic level, by teaching the skills to recruits at the department's own police academy.

Today, and for many years to come, police and other emergency responders throughout the country will require a broad spectrum of both knowledge and operational skills to respond to and successfully manage all types of potentially lethal incidents and events. The CDP training courses also focus on and enhance many of the basic skills needed to help protect the nation's responders from contaminated crime scenes or accidents, and effectively save lives.

The center currently offers more than 40 courses designed for all emergency-response disciplines – and enhances the training with a fiscal bonus: The training provided at the CDP for state and local responders is fully funded by FEMA, a major branch of the U.S. Department of Homeland Security (DHS). Round-trip air and ground transportation, lodging, and meals also are provided – at no cost to the responders or to their various agencies and/or political jurisdictions.

Shannon Arledge is a public affairs specialist at the FEMA Center for Domestic Preparedness in Anniston, Alabama. A retired Marine gunnery sergeant, he served in numerous public affairs/public information assignments during his 20 years on active duty, including tours of duty at Headquarters Marine Corps, the Defense Information School, and Marine Barracks Washington. He deployed twice to the Persian Gulf – in support of Operations Enduring Freedom and Iraqi Freedom – as Public Affairs Chief for Marine Forces U.S. Central Command (Forward) and Public Affairs Chief for the 2nd Marine Aircraft Wing. A graduate of the Defense Information School for Public Affairs and Visual Information, he also has a Bachelor of Science degree in Management from the University of Phoenix.

PERRC GENERAL SESSION PRESENTS

To Stay or Go? What Recent Disaster Events Teach Us about the Decision to Evacuate and the Implications of Doing So

Presenters:

Lewis Soloff, MD

Dan Hanfling, MD

Paul Biddinger, MD

Shelly Schecter, APRN

Ann DeSimone, RN, EMT-B

In this session, participants directly involved with Hurricane Sandy response will offer their experiences, with examples of both pre-event planning and real time problems.

What is the best way to move fragile medical patients when there are limited transportation resources and little time to do so?

How do you decide between moving patients or sheltering in place?

How do you ensure that community partners are available to assist?

Visit Us Online and Learn More
WWW.PERRC.ORG

MAY 8TH - MAY 10TH
ORLANDO, FLORIDA

PERRC

2013 PREPAREDNESS, EMERGENCY RESPONSE, AND RECOVERY CONSORTIUM AND EXPOSITION