domestic preparedness .com

DomPrep Journal

Monthly Edition

US $100 Annual

Volume II, Issue 11

August 2006

Hatred!

How to Respond?

Bomb Squads and HazMat Teams
Teamwork, Cooperation, & Relationships
Brian Geraci, Fire/HazMat, Page 7

Responding to a Suicide Bomber Incident
Robert Stephan, Fire/HazMat, Page 8

Quad State Inititive
Former Fire Chief Lynn Miller
John Morton, Podcast Interviews, Page 10

A Dangerous Disruption
In-Car Police Video Systems Under Assault
Dr. Neil Livingstone, GlobalOptions, Page 5

OSINT Database: Help From the Private Sector
Jennifer Hardwick, Law Enforcement, Page 9

Thomas J. Lockwood, Director, Office of NCR Coordination, DHS
John Morton, Podcast Interviews, Page 19

NIMS and the NCR
Trials & Triumphs at the Operational Level
Joseph Watson, Law Enforcement, Page 12

Two Years Later
The Maritime Transportation Security Act Revisited
Christopher Doane and Joseph DiRenzo III
Coast Guard, Page 14

The New Safety Act Rule
New Opportunities For First Responder Agencies
Brian Finch, Safety Act, Page 16

Telecommuter Security and the Rules Governing Remote Enemy Access
Thomas Kellerman, Cyber Security, Page 17

Project SeaHawk
Building Unity of Effort In Maritime Security
Christopher Doane & Joseph DiRenzo III,
Coast Guard, Page 18

Missouri, Hawaii, Rhode Island, Louisiana, Oregon, and California
Adam McLaughlin, State Homeland News, Page 20

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

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

Staff
Martin Masiuk
Publisher
mmasiuk@domprep.com

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

John Morton
Managing Editor & Interviews
jmorton@domprep.com

Susan Collins
Subscription Mgr. & Layout/Design
subcriber@domprep.com

Sharon Stovall
Web Content Research
sstovall@domprep.com

Paige Dunn
Advertising Sales Coordinator
pdunn@domprep.com

Advertisers in this Issue:

All Hazards Forum

E. J. Krause and Associates

Meridian Medical Technologies, Inc.

RAE Systems

Strategic Research Institute

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

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

Publisher's Message

By Martin Masiuk, Publisher

Both before and during his visit to the Gulf Coast earlier this week to mark the one-year anniversary of Hurricane Katrina, President Bush admitted, several times, that neither the federal government, nor the state of Louisiana, nor the city of New Orleans were fully prepared for the devastation that destroyed much of the Crescent City last year. He also, appropriately, took personal responsibility for the slow and frequently erratic responses of the executive-branch offices and agencies – FEMA (the Federal Emergency Management Agency) was the prime example, of course – that compounded the damage caused by the greatest natural disaster in the nation's history.

Understandably, the president did not dwell on the fact that many individual citizens also were responsible, in varying degrees, for not doing more, ahead of time, to protect themselves, their families, their homes, and their businesses. He focused, rather, on the positive – the fact that all levels of government learned a valuable lesson from last year's hurricanes, are today better organized and equipped to cope with such natural disasters, and will be even better prepared in the future.

There is considerable evidence to back up the president's claim. Some of the particulars are spelled out in this issue of *DomPrep Journal*. Throughout the country, for example, law-enforcement agencies, fire departments, and EMS providers are working more closely together to deal with major disasters – but only in some states, not all of them. Also, various state and local jurisdictions within the greater Washington, D.C., area now work hand in glove with the federal government on a broad spectrum of issues affecting the National Capital Region as a whole. But that multi-jurisdiction/multi-agency approach is still a rarity.

Theoretically, at least, preparing more carefully, and further ahead of time, to deal with natural disasters will make individual cities and states, and the nation as a whole, better equipped to deal with acts of terrorism as well. Here, the evidence is less persuasive. Considerable publicity has been given to the recent apprehension – in England, not the United States – of an estimated 20 or more Islamic fundamentalists alleged to have been planning the in-flight destruction of ten passenger aircraft en route from London's Heathrow Airport to various U.S. destinations. It can safely be assumed that similar mid-air attacks, more carefully planned, will be attempted in the future.

Meanwhile, an attack that was *not* thwarted – the launching of Hezbollah rockets against Israel – not only threatened the peace of the entire Mideast but also demonstrated the grim truth that, in the Age of Terrorism, there is no way to guarantee the safety, health, and continued prosperity of *any* nation, any peace-loving people, anywhere in the world.

This is a lesson that Americans, particularly, should learn thoroughly, and remember always. The United States was taken by surprise by the Japanese attack against Pearl Harbor in December 1941. And by North Korea's invasion of South Korea in June 1950. And by the bombing of the Marine Barracks in Beirut, the attacks on the World Trade Center in both 1993 and 2001, and the simultaneous attacks on the U.S. embassies in Nairobi and Dar es Salaam.

No additional surprises are needed. When, not if, the next attack occurs, the American people will also deserve at least part of the blame if our country is not much better prepared than it now is. In a democracy such as ours, we can--and must--insist on a much higher standard of performance from our elected leaders, at all levels of government, than we have received in the past few years. ▼

About the Cover: Pakistani Shiite Muslims carry pictures of Hassan Nasrallah, head of the Lebanese Shiite militant group Hezbollah, during an anti-Israel protest rally in Lahore on 25 August 2006. Pakistan, which does not recognize the Jewish state, said it would consider participation in a UN force in south Lebanon if its troops were "welcomed" by all parties to the conflict. (Photo by Arif Ali/AFP/Getty Images)

All Hazards Forum

in conjuction with the All Hazards Consortium 501c3

www.allhazardsforum.com

October 10 - 12 | Baltimore Convention Center

Regional Readiness in a Post-Katrina World

2006

Corporate Partners

Founder

IBM

MOTOROLA

Sprint Together with NEXTEL

tyco Electronics M/A-COM

Cisco Systems

verizon business

verizon wireless

TerreStar NETWORKS

Patriot

CSC EXPERIENCE. RESULTS.

Lucent Technologies Bell Labs Innovations

SMART AND ASSOCIATES LLP

Delcan

iTIS Holdings

*As of August 2006

State Partners

A Dangerous Disruption

In-Car Police Video Systems Under Assault

By Dr. Neil Livingstone, GlobalOptions

The highway patrolman was just being cautious when he pulled over the rental truck with a broken taillight as it headed toward Washington, D.C., on Interstate 95. Since the terrorist attacks on the World Trade Center in 1993 and the Murrah Building in Oklahoma City in 1995, law enforcement has given greater scrutiny to rental trucks and similar vehicles. Both of the attacks mentioned involved rental trucks packed with explosives.

As the patrolman approached the driver – a young man with a beard and nervous eyes – a dark object was tossed out of the passenger window. The patrolman was not sure what the “object” was, but it looked to him like a weapon. He instinctively drew his pistol, and seconds later the driver was pressed to the ground, his hands cuffed behind his back. The suspect later was identified as a member of a domestic Hezbollah cell.

A visual image of the incident was captured by a tiny camera mounted on the dash of the patrolman’s vehicle. A majority of patrol cars now are equipped with in-car video systems, which have two purposes: to protect law-enforcement officers from fraudulent claims against them; and to improve agency accountability. The video systems also provide valuable evidence that can be used to prosecute criminals.

Authorities later reviewed the patrolman’s video, which clearly showed the driver trying to get rid of evidence by throwing a gun out of the rental truck. The case has yet to go to trial. But if new regulations proposed by the International Association of Chiefs of Police (IACP) are enacted, the driver could be set free. So could hundreds of other criminals, some of them already convicted.

Good Intentions Gone Awry

The scenario described above, although based on numerous real-life cases, is imaginary – but the proposed IACP regulations, and the harmful consequences that would result, are very real. The ability of law-enforcement agencies throughout the country, at all levels of government, to fight crime – and, not incidentally, the war on terrorism – will be dealt a severe blow if the proposed IACP regulations for in-car video systems are not modified.

What happened is this: With the best of intentions, the IACP created a committee in 2004 to establish minimum performance specifications for in-car video systems. The original goal was to enhance police safety, but it has gone far beyond that. A comment period ends on August 31, after which the IACP is expected to issue final regulations.

Among the specifications being recommended is a requirement that all new in-car video systems be equipped with high-resolution cameras (4CIF). At first glance, that requirement might seem reasonable – but making it mandatory at all times and in all situations will cause chaos in police stations and courtrooms throughout the country.

A rigid insistence that only new, higher-resolution 4CIF cameras will be acceptable in the future will make the older video systems now installed in police cars seem inadequate. For that reason it is almost certain that defense attorneys will argue that video captured by the earlier in-car systems should be ruled as insufficient evidence, and will be able to cite the IACP as the defining authority.

The immediate result will be that hundreds of upcoming cases involving in-car video imagery will be jeopardized. Much worse, though, is the likelihood that many police departments may decide to scrap their present in-car video systems on the grounds that the visual evidence provided by those systems cannot be used in court.

Making the problem worse is the fact that the nation’s police forces already are having difficulty purchasing video systems for their vehicles because of the high cost of those systems. The new 4CIF systems mandated by the IACP will be even more expensive, which means that many police departments will be unable to purchase video systems for their patrol cars.

A Clause and a Declaration Both Needed Quickly

There is, fortunately, a quick and affordable solution to this problem – namely, that the shortcomings in the specifications proposed can be easily avoided if the IACP would simply include a grandfather clause that permits the continued use of existing in-car video systems for a reasonable period of time. To do this, the IACP must specifically declare that the systems currently in use are acceptable and that the video recordings produced by these systems are sufficient for submission as evidence in a court of law on a case-by-case basis, just as they have been in the past.

It also is essential for the IACP to provide a transitional period – perhaps two years – to implement the new specifications. It is questionable whether any company now in the video business can immediately meet the proposed IACP specifications for an in-car 4CIF system. As with other new or improved products of any type, it will take time to design, test, evaluate, produce, and distribute the new systems. In the meantime, without a transitional period, law-enforcement agencies will not want to purchase any in-car video system that does *not* meet the new standards. Current contracts and budgets will be thrown into disarray, and precious months might well pass before *any* new systems are available for purchase.

There is no reason to cause such disruption to law enforcement, the courts, and the video-system manufacturers. Permitting – or, better, mandating – a two-year period before the IACP specifications go into force would ensure a smooth transition. It already has taken nearly two years to draft the specifications, so another two years before implementation would not be unreasonable, particularly given the complexity of the technology involved.

During the transition period, law-enforcement agencies would be able to change over to the new technology without any significant disruptions. Of much greater significance is that existing equipment would not be made obsolete overnight, court cases would not be jeopardized, and, most importantly, law-enforcement safety would not be impaired.

The battleground against terrorism is being fought on many fronts. As the nation focuses greater attention on terrorist threats, care should be taken that current law-enforcement tasks are not neglected and that police forces have the tools they need to get their job done. In the preceding scenario, the driver was a Hezbollah member. Disrupting that and similar organizations, and keeping their members behind bars – even if "only" on a firearms charge – could be critical to winning the war on terrorism.

A few other reasons why the IACP specifications for in-car video systems must be modified:

- Technologies Overly Complicated and Unaffordable – The proposed specifications require that the new in-car video systems being designed incorporate many complicated and expensive technologies. Many police forces prefer systems that are less complicated but more reliable--and less expensive to operate.
- Anti-Competitive in Nature – The proposed specifications direct law-enforcement agencies to purchase the new in-car video systems only from companies that are already manufacturing systems. Prototype systems are prohibited. This mandate unfairly prevents new companies from entering the market and makes it less likely that innovative technologies will be incorporated to reduce expenses and improve performance.

Neil C. Livingstone is CEO of GlobalOptions Inc., an international risk management and business solutions company headquartered in the nation's capital. He has authored nine books on terrorism, national security, and foreign policy, has written more than 180 articles in leading homeland defense publications, and is a veteran of more than 1,100 television appearances.

Bomb Squads and Hazmat Teams

Teamwork, Cooperation, and Relationships

By Brian Geraci, Fire/HazMat

The squad leader is back at work from a well deserved family vacation. The previous shift has been relieved and the squad's activities during the past week have been reviewed. Just as the morning equipment check is finished a call comes in warning about a "suspicious package" reported to have been left on the elevated platform of a subway station nearby.

While the bomb squad is on its way to the station another call comes in from the dispatcher, warning that the package is leaking and that a noxious odor also has been detected. The dispatcher reports that Fire/Rescue personnel, including a hazardous materials response team, also is en route to the scene.

A Warm Handshake, And Reasonable Hopes

All of the units responding arrive at the station in the next several minutes – and, surprisingly perhaps, the bomb squad commander and the hazardous-materials operations chief meet one another for the first time. The bomb squad commander tells the hazmat chief that his bomb technicians cannot enter the site because of the leaking package, and the hazmat chief says that his people also cannot go onto the platform because of the possibility that the "package" may be a bomb. Meanwhile, all subway and rail lines in or headed to the area are shut down.

Five years after the worst terrorist attacks against American citizens in history, on U.S. soil, and with almost daily reminders of terrorist activities elsewhere in the world, it might reasonably be hoped that scenarios such as that described above are extremely rare. And, in fact, community bomb squads and hazmat teams across the nation have taken several steps forward to ensure that such frustrating scenarios do *not* occur. Numerous bomb technicians throughout the United States already have gone through WMD (weapons of mass destruction) training and are now required to qualify as hazardous material technicians prior to attending the Federal Bureau of Investigation's Basic Hazardous Devices School in Huntsville, Alabama.

In addition, new and improved protective clothing – including a "level B" ensemble with an explosive search suit as an over-garment – has been developed to allow bomb technicians to work more safely as well as more effectively in a hazardous environment.

The search suit does not afford the bomb technician the same full protection provided by a complete bomb suit, but it does afford a certain degree of blast protection, and bomb suit manufacturers are currently working on improving and expanding the level of blast protection provided.

It Starts With a Phone Call

But the real key to developing a closer and more productive joint effort between bomb squads and hazmat teams is not updating the training provided or even the purchase of new equipment – it is, more than anything else, creating the necessary working relationships and partnerships between the bomb squads and hazmat teams *prior* to their participation in real-life operational incidents such as that described above.

The development of such relationships can sometimes be difficult, of course, particularly if the bomb squad is a law-enforcement unit and the hazmat team works on the fire side of the house. Regardless of the institutional relationships, and despite what is implied by the organization charts, the commanders of both teams must meet together, early and often, to discuss and resolve any operational issues ahead of time. Following that, the bomb squads and hazmat teams must really work and train together as one team.

There are many situations – not only bomb calls but also drug lab incidents and other special non-emergency events – in which both teams will have to work together from start to finish, and the number of such situations is increasing rapidly. Taxpayers have the right to expect a synergistic improvement from the cooperative efforts that will be necessary to defend the community.

In Montgomery County, Maryland, the two types of teams are partnered within the fire department, and that organizational relationship has made it easier for the members of both teams to train together and work together. Bomb technicians not only train frequently with the hazmat team but also go through an annual hazmat technician recertification. Similarly, members of the hazmat team respond to bomb calls as part of their own job, not only to provide support to the bomb technicians and to the overall operation, but also – if by chance an unknown substance is detected – to assume responsibility for operations within their own areas of expertise. The fact that bomb and hazmat incidents are managed in much the same way – with control zones established, special protective clothing and specialized equipment used, and similar command structures in place – helps significantly in dealing with such incidents.

It obviously makes sense that the two types of teams work and train together to ensure a safe and positive outcome of various incidents threatening their home communities. And it is encouraging that there already are many jurisdictions across the country where the two types of teams have joined forces and are working together with increasing effectiveness. In communities where this is not the case, bomb squad leaders and hazmat team commanders would be well advised to take the time now to make the initial call that will start developing the improved working relationships needed. By doing so, these unit leaders will ensure that the next operational incident will be better coordinated, the safety of all response personnel under their jurisdiction will be enhanced, and the communities they serve will be both safer and more secure than they now are.

Brian Geraci is a Battalion Chief with the Montgomery County Fire and Rescue Service, Montgomery County, Maryland. He is presently assigned to Montgomery County's Homeland Security Department. Chief Geraci has over 30 years of service in the county and was a charter member of the county's Hazardous Incident Response Team and served as one of the team leaders.

Responding to a Suicide Bomber Incident

By Robert Stephan, Fire/HazMat

As has been proved literally hundreds of times in Iraq, Israel, and elsewhere, the detonation of an explosive device by a suicide bomber can occur, without warning, anywhere in the world – including the United States. When, not if, such an attack takes place on American soil, the jurisdiction directly victimized will be expected to be fully prepared to deal with it. More specifically, the community's first responders – firefighters, police officers, and emergency medical technicians, primarily, who will in all likelihood be the first trained personnel on the scene – must be trained and ready to save lives, stabilize the incident scene, and minimize the short- and long-term impact of the suicide bombing in general.

Those who activate the explosive device will pick the date, time, place, and method of attack – and may decide to maximize the destructive effect by lacing their weapon with an extremely toxic chemical or radioactive material, making it a so-called "dirty bomb." Because of this possibility, responders who are approaching the scene should position themselves upwind and wear an acceptable level of personal protective equipment, including respiratory protection devices. Caution in obviously necessary – but so is speed. It is particularly important, for example, that the first emergency responders on the scene enter the incident area as rapidly as possible to immediately remove any injured patients.

Thanks in large part to the efforts of U.S. and allied intelligence agencies, there have been no new terrorist attacks on U.S. soil since the bombing of the World Trade Center, and the Pentagon, on 11 September 2001. It is only natural, therefore, as time passes, that memories fade and the nation's first responders are lulled into a false sense of security and the belief that another 9/11 event either will not occur or, at worst, is very unlikely. That sense of complacency may well be the first responders' greatest enemy.

Last Week, and Five Years Ago

Several other incidents of self annihilation by terrorists have in fact been attempted. The arrest last week of the terrorists plotting to carry out a dozen or more suicide bombings on U.S. passenger aircraft en route from London's Heathrow Airport to the United States was a helpful reminder that as far back as December 2001 Richard Reid, a British citizen, had planned to detonate a shoe bomb containing plastic explosives while over the Atlantic Ocean on a commercial flight from Paris to Miami.

First responders who are trained in managing mass-casualty incidents, and in patient triage, may believe that they are now properly prepared – much more so, certainly, than in September 2001. But U.S. decision makers, and the American people, are entitled to ask if the nation's first responders are, in fact, truly prepared for the grotesque mutilation, carnage, dismemberment, and repulsive odors emanating from the explosion site that will be facing those who are treating the victims of a suicide-bomb attack.

The successful attack, by American citizens, on the Murrah Building in Oklahoma City, was not a suicide attack per se – but it proved that there are few if any public buildings or critical-infrastructure facilities within the United States that are 100 percent safe from terrorist attacks in general. Suicide attacks, by definition, are more difficult to guard against than attacks in which the terrorists themselves hope to survive. And it is obviously more difficult to protect any community from several attacks occurring more or less at the same time. In short, well-planned and well-implemented multiple attacks by suicide bombers similar to the attacks against the public transportation systems in London, Madrid, and Mumbai could occur in the United States as well.

Immediately If Not Sooner

Gary Briese, executive director of the International Association of Fire Chiefs – and, not incidentally, one of the nation's earliest prognosticators of the probability of terrorist attacks within the United States itself – subscribes to what is called the "20 minute rule" for the care and evacuation of patients. The approach suggested by Briese, and many other experts, emphasizes that the victims be removed from the bomb site, and the incident scene, as quickly as possible – i.e., within 20 minutes or less – and be transported to the closest available trauma center. To meet that ambitious goal, though, hazmat responders must rapidly enter the explosion site to verify the presence (or, preferably, absence) of possible WMD (weapons of mass destruction) materials, a difficult task that requires the use of specialized detectors. If such materials are present, decontamination of the site will probably be necessary.

For operational purposes, perhaps the most important question that will be asked, if and when a suicide bomb explodes in a crowded venue, is what the first incident commander arriving on the scene should decide about victim rescue. If he or she decides – because of the *potential* presence of a secondary device – *not* to proceed immediately into the debris field to rescue and remove injured victims, the question is still valid: At what point in time will such a decision be made and carried out? The time for preplanning responders' incident activities, and for developing operational guidelines, has to be *prior* to an incident, not after another suicide bombing takes place.

Following are some suggested action guidelines for first responders arriving at the scene of a suicide bombing or similar incident:

- Approach and position themselves upwind, 300 feet or more from the edge of the debris field;
- Isolate the area and deny entry by those who are not first responders – and by first responders who are not wearing the personal protective equipment they need;
- Search the incident area as rapidly, as safely, and as thoroughly as possible for secondary suicide bombs and/or other explosive devices;
- Immediately – i.e., in 20 minutes or less – remove injured victims and transport them to an appropriate medical facility; and
- Extinguish any uncontrolled fires in the area.

Battalion Chief Robert Stephan, a member of the Montgomery County (Md.) Fire and Rescue Service for 34 years, has been the leader of the county's Hazardous Incident Response Team since its creation in 1981. He is also a member, and a former chairman (for 14 years), of the HazMat Subcommittee of the Metro Washington Council of Governments for the National Capitol Region. He is cross-trained as a 15-year National Registry Paramedic, a member of the Washington, D.C., National Medical Response Team, and an instructor for the National Center of Biomedical Research and Training.

OSINT Databases

Help From the Private Sector

By Jennifer Hardwick, Law Enforcement

On 28 July 2006, a Pakistani-American man went on a shooting rampage at the Jewish Federation in Seattle, Washington, killing one woman and injuring five others. In a statement to an emergency dispatcher, the shooter discussed his motivation: "These are Jews and I'm tired of getting pushed around and our people getting pushed around by the situation in the Middle East."

This horrific incident illuminates the critical mission of the burgeoning open-source intelligence (OSINT) industry: monitoring global events through non-classified channels and translating them into actionable intelligence for clients, be they multinational businesses, academia, the government, or the emergency-responder community. For the past several years, OSINT experts have been translating what the shooter means by "situation in the Middle East" into a coherent context with anticipatory threat assessments. In short, OSINT aids both in the prevention of, and response to, terrorist and criminal operations.

As demonstrated by the shooting in Seattle last month, the still unresolved crisis in Lebanon between Hezbollah and Israel is critical for U.S. emergency responders to understand. Use of an OSINT database will put the crisis into perspective, typically offering near-real-time updates to significant developments. OSINT can provide an informed forecast, for example, on whether Hezbollah – a more sophisticated international terrorist network than al-Qaeda is – is likely to launch terrorist attacks against Israeli interests abroad. Or perhaps against American interests, almost anywhere in the world, because of the perceived U.S. support of Israel.

Incidents Both Real and Simulated

In either case, such attacks would seem to be unlikely – unless or until Hezbollah leaders are assassinated or Hezbollah's existence as an armed militia is legitimately threatened. Should either of these two developments occur, U.S. emergency responders would be notified through subscriptions to OSINT services. Security postures around Israeli or Jewish centers then would be heightened and security officers – now armed with additional situational awareness – would be more attuned to suspicious behavior around high-value targets.

> ***For the United States to wear blinders because it shares land borders with only two other countries is a culpable abdication of responsibility***

Case studies for the preceding scenario can be drawn from the 1992 bombing of the Israeli Embassy in Buenos Aires, Argentina, in reprisal for the assassination of Hezbollah leader Sayyad Abbas Musawi, and from the 1994 Jewish community center bombing, also in Buenos Aires. In the latter incident, it is worth noting, the lead bomber was a former resident of Detroit, Michigan.

The benefits derived from the use of OSINT sources may perhaps be best illustrated by imagining a hypothetical terrorist incident involving Islamic extremists exploding a so-called dirty bomb in an urban area anywhere in the world. Three benefits derived from the availability of OSINT services would immediately follow: (1) Emergency responders, specifically fire fighters and hazmat teams, would be quickly notified of continuing developments and of similar incidents that have occurred; (2) Law-enforcement agencies would be provided detailed information about the members of the organization alleged to be responsible for the attack (e.g., their nationality, motivations, modus operandi, group dynamics, and – perhaps the most important information needed – whether they take hostages or simply kill those they have captured); (3) Hospital emergency personnel would be made aware of the possibility of contaminated patients seeking treatment – and, therefore, of the need for triage centers with decontamination capabilities to be opened to receive such victims.

In providing these and other notifications, it is worth pointing out, OSINT would be simultaneously supporting the emergency operations of each of the three main subtypes of emergency responders: fire fighters, law-enforcement personnel, and emergency medical service technicians.

Independent International Expertise

The geo-political risk services offered by OSINT do not compete with news organizations, it should be emphasized, or with domestic and international government sites; they complement them. Independent OSINT firms – with international scope – retain qualified regional and topical experts to analyze political events as they unfold and put them into a context that an action officer can use to move forward effectively to meet specific requirements and goals.

Signing up for news alerts is a good start for agencies and organizations considering the use of OSINT services, but emergency responders simply require more in-depth intelligence than that. Fortunately, the FY 2006 Authorized Equipment List (AEL – the list that the Department of Homeland Security (DHS) relies on for funding equipment and services) may allow first responders to use DHS Grant Program funds to purchase OSINT databases.

In November 2005, the federal government itself recognized the utility of OSINT by standing up the national Open Source Center (OSC) in suburban Virginia not far from Washington, D.C. The OSC, which is similar in many respects to other multi-agency national intelligence centers, is built upon the legacy agency known as the Foreign Broadcast Information Service.

John Negroponte, the Director of National Intelligence, has been quoted as describing the OSC as the "centerpiece … for the Intelligence Community to devote more attention and resources to exploiting openly available information."

OSINT services are both web- and email-based and require passwords or IP-recognition to access. Leading OSINT services also can be commissioned for customized, tailored reports that emphasize specific needs and interests. These services can be used by incident commanders constructing community response plans, bomb squads interested in new developments in improvised explosive device (IED) technology, customs agents learning of an imminent attempt by terrorists to cross the border, or even emergency medical personnel preparing their triage centers for a chemical, biological, radiological, or nuclear (CBRN) response.

A Culpable Vulnerability

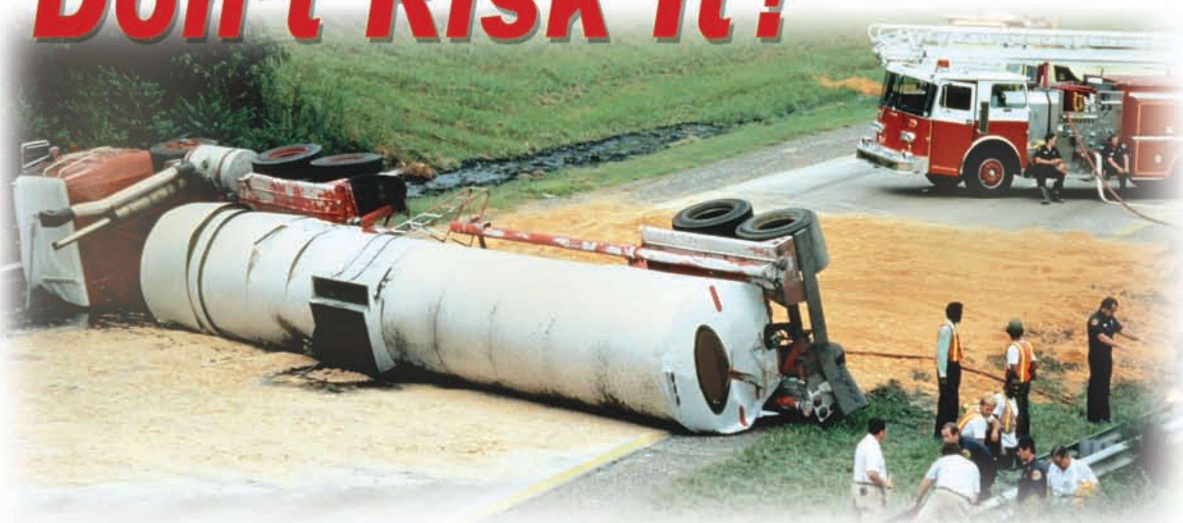
OSINT providers often also release special reports and bulletins explaining late-breaking emergency news or focusing on less time-sensitive issues. Following are a few titles illustrating the scope and breadth of such reports: "Hazardous-Materials Trucks: Terror Threat?"; "U.S.-Mexican Border as a Terror Risk"; "Canada Pinches Tamil Tigers' Pocketbooks"; and "Jihadist Recruitment in U.S. Prisons."

OSINT services have become increasingly essential for emergency responders. Transnational crime is increasing rapidly, national borders are becoming almost irrelevant, and the lessons learned from one incident in one part of the world can prove invaluable in the prevention of similar incidents elsewhere. What happens in one city is often plotted for or repeated in another: Madrid, London, Mumbai, and New York, to list just a few obvious examples. For these and a host of other reasons, emergency responders must be given the tools they need – particularly and specifically in the information field – to fully understand the complex issues and developments occurring globally.

It may be trite, but it is nonetheless true, that there is no "safe" country anymore. Many countries have and/or harbor domestic and international terrorist organizations. Many have little or no control of subversive groups (which also may have cells within the United States). Many have porous and largely uncontrolled borders. And many have less than pro-U.S. agendas. Still other nations are led or governed by paramilitary enforcers controlling media and society.

In short, each country is influenced by its neighbors, and for the United States to wear blinders because it shares land borders with only two other countries – both of them friendly (in most important matters) to U.S. interests – is a culpable abdication of responsibility that leaves the American people vulnerable to networks of international criminals and terrorists.

Jennifer Demmert Hardwick is the Senior Director for Intelligence and Analysis at the Terrorism Research Center Inc. (TRC). She manages a web-based intelligence service that supports client decision making and global operations. TRC is a best-of-breed provider of intelligence, analysis, training, and operational support for public and private clients worldwide.



NIMS and the NCR

Trials and Triumphs at the Operational Level

By Thomas Watson, Law Enforcement

Creation of the National Incident Management System (NIMS) – which requires federal, state, and local jurisdictions to work together during and in the aftermath of what are called incidents of national significance – has done much to improve the working relationships between and among first-responder agencies and organizations in neighboring states or municipal jurisdictions. There have, of course, been some implementation problems, but more and more agencies are in fact purchasing the same equipment, using the same communications systems, and training together.

The goal of these and other cooperative efforts is to facilitate the intergovernmental joining of various emergency-services communities within the same general geographic area into a cohesive whole that would synergistically upgrade the emergency-preparedness capabilities of the entire region. In that context, it is worth studying the successful real-life example of a major, and very recent, multi-jurisdiction effort that demonstrated an extraordinary – perhaps unprecedented – level of cooperation among not only a broad spectrum of federal, state, and local government agencies but also across several functional first-responder disciplines, specifically including but not limited to law-enforcement agencies, the fire services, and emergency medical services units and personnel.

That well-publicized effort concluded earlier this year with the sentencing – in the U.S. District Court for the Eastern District of Virginia – of convicted terrorist Zacharious Moussaoui. The fact that the sentencing proceedings went so well – i.e., without major disruptive incidents – was due in large part, it is reasonable to suggest, to careful and extremely detailed planning by a host of federal, state, and local agencies with overlapping missions and responsibilities in the greater Washington, D.C., area – also known, for operational purposes, as the National Capitol Region (NCR).

It is not the presence of numerous federal, state, and local jurisdictions within the same geographic area that gives the NCR its unique status but the fact that the region is home to the executive, legislative, and judicial branches of the U.S. government and to hundreds of federal offices and agencies, large and small. Almost any major event or incident that occurs within the National Capitol Region has national and, usually, international repercussions.

The Aftermath of an Airplane Crash

It was not the terrorist attacks of 11 September 2001 that led to the creation of the NCR but an earlier disaster – namely, the Air Florida crash of 1982, which led to formation of the Washington's area's Metropolitan Council of Governments (COG). Over the past two decades the COG has, despite some areas of disagreement, initiated a number of innovative multi-jurisdiction programs and achieved an uncommon degree of success in regional planning and the implementation of mutual-aid agreements.

Working through numerous committees – with jurisdiction, for example, over law-enforcement and/or fire-service matters, or HazMat issues, or local transportation problems and resources – COG developed and, of particular importance, reached agreement on many region-wide plans that, to be successful, required the cooperation of many agencies from a multitude of political jurisdictions throughout what was evolving into today's National Capitol Region.

COG's long-term experience in both planning and, of equal if not greater importance, training – without which the most perfect planning would not be effective – gave the region a long leg up in emergency-preparedness planning in general. The region-wide response to the 9/11 attack on the Pentagon served as an acid test that demonstrated both the significant strengths in regional emergency services cohesion that had been developed as well as the many difficult challenges that still remain.

Inter-Agency Cooperation And Interoperability

The Moussaoui trial provided another but in many respects different challenge, as well as the opportunity to develop and validate intergovernmental integration plans and preparedness capabilities over a longer period of time. The high-risk legal proceedings, dubbed Operation Enduring Justice, required close and continuing cooperation from, among other offices and agencies, the United States Marshals Service, the U.S. Attorneys Office, the FBI, the U.S. Department of Homeland Security, and the Federal Protective Service as well as the City of Alexandria's Police and Fire Departments, and Sheriff's Office, and the Fairfax County Police Department. At some points during the proceedings there were as many as eighty personnel manning key positions on the ground, with others flying air cover overhead and still others assigned to the unified command-and-control center that had been established. A multi-unit intelligence cell also supported the event.

Protective and critical incident-response measures were planned ahead and carried out by interagency interior and perimeter security personnel, rapid-response special operations and hazardous materials teams, and various tactical and counter surveillance units. Because of the increased threat posed by the potential use of improvised explosive devices (IEDs), full route security was provided for the daily movements of the defendant between the courthouse and the Alexandria Adult Detention Center.

Planning and Training Emphasized

The interagency planning for the proceedings started four years ago and continued from the defendant's initial court appearance to, through, and beyond the actual sentencing.

The original interagency planning team evolved into a working group that met monthly to resolve various training and operational issues. The interagency team also reviewed individual agency operations plans to guard against a confliction of responsibilities and ensure the operational cohesion of the participating agencies involved.

Training was emphasized throughout, and included not only tabletop exercises but also two dynamic modeling and simulation exercises (using the "EPiCS" tool provided by Advanced Systems Technology). The principal lessons learned from the simulation exercises were incorporated in later operational plans, with improvements added when and where needed. The final training event, not too long before the start of the trial, was a full boots-on-the-ground exercise.

Special-operations teams, Haz/Mat-response units, and EMS personnel had full access to the U.S. Courthouse. The result was an unprecedented level of intergovernmental, multi-disciplinary situational awareness of the venue. During and following the preliminary training and robust final exercise, operational plans were constantly strengthened across both governmental and functional disciplinary lines.

Dealings With the Public & the Media

Because of the U.S. Courthouse's close proximity to residential buildings, commercial businesses, and other federal buildings, a concerted effort was made to educate local residents and businesses about the impact of such a long-term event on their own lives and livelihoods. To allay community concerns and uncertainty, such issues as traffic, parking, noise, safety, construction schedules and disruptions, and civil disturbances were fully and repeatedly addressed. In large part because of these effective community-outreach initiatives, local residents felt a part of the total security and protective operation, as evidenced by the large number of calls placed to the Alexandria Police Department warning of suspicious activity in and around the U.S. Courthouse.

From the start, communications interoperability was one of the most pressing concerns that had to be addressed. Fortunately, the NCR already had in place a reliable system known as the ACU-1000 (as well as a portable version, the TRP-1000 – provided by Raytheon JPS). Those systems facilitated interagency communication and permitted the use of each agency's own communications equipment in an encrypted mode, regardless of megahertz range or the type of system used. (The system is currently available throughout the NCR for other region-wide uses. Work continues, however, on the development of secure voice-over Internet protocols that will both provide a system without barriers or boundaries as well as a redundancy in work stations.)

Media coordination, another type of communications concern, began several months before the start of the trial. The application of American justice to one of the co-conspirators of the 9-11 attacks generated worldwide media interest, with over a hundred print and broadcast outlets expressing a desire to cover the event. A close liaison was developed between the media elements and the public affairs offices of the various agencies participating. The effectiveness of this interagency-media working relationship is perhaps best demonstrated by the fact that there were very few incidents of press attempts to violate security protocols. In fact, there were some instances in which members of the media themselves alerted federal and local police officers of suspicious activities that were taking place.

To summarize: Although the Moussaoui trial was not a no-warning WMD (weapons of mass destruction) incident, it had the potential of becoming one by attracting a major terrorist attack. The long-term sustained preparedness requirement for the operation undoubtedly stretched local resources to the limit. It was successful in that there were no security breaches and that the region's responders were able to show the surrounding community that the many agencies involved could plan, coordinate, communicate, and carry out a long-term event with multiple agencies operating seamlessly with one another.

During the course of the sentencing proceeding, interestingly, a Congressional committee was holding hearings during which the ability of federal, state, and local agencies to communicate and operate in a cohesive manner was being seriously questioned. It was coincidental, but ironic, that those hearings about the NCR's emergency-preparedness capabilities were taking place at the same time that an ongoing operation was demonstrating an unprecedented level of effective intergovernmental operational preparedness in the community of Alexandria, Va., only a few miles from Capitol Hill.

Sergeant Joseph Watson is a former Marine Military Police Officer and 25 year veteran of the City of Alexandria Police Department. Currently team leader for the Department's Special Operations Division, Community Support Section Homeland Security Unit. He is the founder and President of Special Operations Solutions, LLC. Consulting, Planning, Training, Exercises and Operations.

Two Years Later

The Maritime Transportation Security Act Revisited

By Christopher Doane and Joseph DiRenzo III, Coast Guard

The requirements of the Maritime Transportation Security Act (MTSA) of 2002 – which was specifically designed to strengthen security in U.S. ports – became effective on 1 July 2004. The primary responsibility for implementation of the MTSA regulations was assigned to the U.S. Coast Guard. Two years later, experts in maritime security both in and outside of government are taking a long second look to see how implementation has progressed and what work remains to be done.

By the time the MTSA-mandated regulations went into effect just over two years ago, the Coast Guard already had approved 44 area maritime security plans (which govern the overall security of U.S. ports), approximately 3,100 facility security plans, and 9,500 vessel security plans. Approving the plans was only the first step, though; the plans also had to be implemented by the various stakeholders in each of those plans.

An exercise program to test the area plans also had to be developed, and facility and vessel security verification programs also had to be established, and implemented, to ensure compliance with the plans. Finally, a means to ensure continual improvements as and when needed had to be created and implemented.

Tests, Exercises, and Evaluations

To test the area plans, the Coast Guard – working in close cooperation with the Transportation Security Agency (TSA) – initiated the Port Security Training Exercise Program, or PortSTEP. The two agencies agreed on a schedule to conduct 40 PortSTEP exercises between August 2005 and October 2007 to evaluate the ability of federal, state, and local agencies to execute a unified and effective response to a transportation security incident (TSI).

Port exercises usually take two forms: table-top exercises, during which representatives of the stakeholder agencies participate in a facilitated discussion to decide on how they would respond to a particular scenario (provided to them as part of the exercise); and full-scale, hands-on, almost-real-life exercises in which the agencies participating would actually deploy their forces in response to a given scenario. If all goes well, the lessons learned from the two types of exercises are used to update the port's security plan.

To verify implementation of the vessel and facility security plans, the Coast Guard has initiated and is carrying out a security compliance program, which consists both of annual compliance visits and – either when a breach of security occurs, or because of observations during other Coast Guard interactions with industry – unscheduled evaluations of security adequacy. The corrective actions taken when problems have been discovered have ranged from a temporary halt of security operations at the facility or vessel to the issuance of formal notices to owners and/or operators to correct existing deficiencies in their plans.

> *Approving the plans was only the first step; the plans also had to be implemented by the various stakeholders*

Diplomacy Needed For International Cooperation

Another key MTSA requirement assigns responsibility to the Coast Guard to conduct foreign port security assessments. To carry out that important but highly sensitive mandate, the Coast Guard established an International Port Security Program that uses both liaison officers (each of whom is assigned a portfolio of other nations with which they develop working relationships) and port visit teams, the members of which visit U.S. trading-partner nations to share port security practices and observe port security measures. More than 50 countries – representing the "last ports of call" for over 80 percent of the vessels arriving in U.S. ports – have been visited since the start of the program.

The actions already taken represent obvious and frequently impressive progress in implementation of the Maritime Transportation Security Act, but even those in charge of the various programs listed above say that there is still much more to be done. Moreover, several other important programs and projects – e.g., the Transportation Worker Identification Card (TWIC) program, the Enhanced Crewmember Identification/International Seafarers Identification program, the Automatic Identification System (AIS) project, and the Long Range Vessel Tracking/Identification System project – are still in various stages of planning, funding, and implementation and must be evaluated periodically for the foreseeable future.

There is general agreement in the maritime community that all of those major programs should be implemented just as quickly as possible. Another step that should be considered, the experts say, is a new round of port, facility, and vessel vulnerability assessments to evaluate the MTSA's effectiveness in reducing overall maritime risk.

Christopher Doane and Joseph DiRenzo III (pictured above) are retired Coast Guard officers now serving as Coast Guard civilian employees; both also are Visiting Fellows at the Joint Forces Staff College. Although management experts in and out of government were consulted in the preparation of this article, the opinions expressed in the article are their own.

DomesticPreparedness.com: Home

http://www.domprep.com/

Domestic Preparedness.co

DomPrep Journal
Online Edition

Email: Password: Log In Not a member? Forgot password?

Find articles containing Search Advanced Search

- Home
- First Responder
- Medical Response
- Updates
- Audio Interviews
- Military Support
- Borders & Ports
- Commentary
- Funding and Regulations
- Cyber Security
- Resilience
- Print (PDF) Version
- Calendar
- WebConferences
- Online Exhibits
- Contact Us
- Advertise

Medical Response

Triage Strategies for Hazardous Materials Mass-Casualty Incidents What are the best indicators of victim survivability? The RPMs provide a few clues that can be used to START processing. But continuing updates and additional analyses are needed to improve the decision-making process. read

Preparing to Cope With a Pandemic Flu There are several ways, none of them easy–or 100 percent certain–to fight a pandemic that could kill hundreds of thousands of everyday citizens. The Los Alamos project suggests that the first-responder focus should be on vaccinations. read

Reports

President Bush Announces the National Strategy for Pandemic Influenza Implementation Plan "[The] — Federal Government has begun strengthening our ability to safeguard the American people in the event of a devastating global pandemic and helping to prepare the Nation's public health and medical infrastructure." President George W. Bush read

Hurricane Katrina: A Nation Still Unprepared - A Report Released by the Senate Committee on Homeland Security and Governmental Affairs This report has four major sections: a narrative of what happened; findings; recommendations for changes;and appendices. The report recomends that FEMA be abolished and replaced with a new agency within the Department of Homeland Security. read

GAO (Government Accountability Office): Department of Defense (DOD) Needs Consistent Policies and Clear Processes to Address the Survivability of Weapon Systems Against Chemical and Biological Threats GAO is recommending modifications to DOD's current weapon system acquisition policy to ensure that weapon system chemical and biological survivability is consistently addressed. read

Government Update

DHS Implements Immediate Measures to Secure Access to Ports "It is fundamental that individuals who pose a security threat do not gain

EMS

Tags of Survival: The Start System The triage goal is to maximize the number of lives saved. But to do so requires some extremely difficult decisions from the EMT on the scene, particularly in mass-casualty incidents when time is limited and information is in short supply. read

EMS Hazardous Duty: Not for the Meek The members of EMS units are among the first to respond to major disasters in their home communities. They also are on the front lines of danger, particularly in HazMat incidents, and for that reason alone must be among the best prepared & protected. read

When seconds matter, Meridian's Auto-Injectors meet the challenge of emergency drug delivery.

MERIDIAN MEDICAL TECHNOLOGIES

For More Information

State Homeland News

Texas, New York, and Maine Texas conducts a pre-season hurricane exercise at Disaster City training complex. New York City upgrades communications systems in ambulance and FDNY vehicles. And Maine moves forward in tri-state planning for major disasters. read

Maryland, Wisconsin, and Alabama Disaster exercise: Maryland airport demonstrates preparedness capabilities, & communications gap. Wisconsin deals with the potentially "devastating"

Subscribe Today

Management Solutions

Technology Solutions

Best Practice Solutions

Fire/HAZMAT • Law Enforcement
EMS • State Homeland News • Coast Guard
Military Support • Transportation Analysis
Audio Interviews • Maritime Security • Public Health
Military Medicine • Hospital Administration

Integrated Solutions

domestic preparedness .com

DomPrep Journal

US $75 Annual

Volume II, Issue 5, March 8, 2006

RUN! But Where?

Isolation & Quarantine: How, When, and How Much
Jerry Mothershead
Military Medicine, Page 5

Dennis Atwood, Program Manager MMRS
John Morton
Interviews, Page 6

Evacuation Planning: A Long Way To Go
Joseph Cahill
EMS, Page 8

The Role of Medical Systems in Homeland Defense
Michael Allswede
Hospital Administration, Page 12

Missouri, Tennessee, And California
Adam McLaughlin
State Homeland News, Page 15

For more details, visit:

Knowledge Delivered Digitally in Either Printable PDF or HTML

Providing You with Solutions Weekly

Authored by Practitioners with day-to-day Operational Knowledge

Subscribe now to DomPrep Journal US $100 Annual • Email: subscriber@domprep.com

FREE to Qualified Professionals

domestic preparedness .com

DomPrep Journal
Management Solutions

410.518.6900
www.DomPrep.com

The IMR Group, Inc., publishing DomesticPreparedness.com (DomPrep) since 1998 to integrate the diverse first-responder communities of state, local, and federal preparedness communities. Most recently, the reach was extended to include building-facility managers and critical-infrastructure, maritime, borders, ports, and public-health officials and operators.

The New SAFETY Act Rule

New Opportunities for First Responder Agencies

By Brian Finch, Safety Act

The so-called "SAFETY Act" – officially known as the Support Anti-Terrorism by Fostering Effective Technology Act – of 2002 is an important tool in the ongoing efforts to make useful technologies and services more quickly available to the nation's first-responder community. One reason the Act was created was to give the companies providing anti-terror services and/or technologies the opportunity to receive the liability protection they need to continue in business.

The Department of Homeland Security (DHS), which provides the liability protection, promised from the beginning to continually improve the SAFETY Act application process, and it has done so – most recently by issuing a new SAFETY Act Rule that includes a number of helpful changes designed to make the process both less cumbersome and less expensive and, at the same time, easier both to understand and to implement.

> **The Act was created to give companies providing anti-terror service and/or technologies the opportunity to receive the liability protection they need**

To begin with, the new Rule offers some exciting possibilities for greater use of the SAFETY Act by consumers of anti-terror products and services at all levels of government. First-responder agencies and organizations should be particularly aware of the improved ability they now have to link their procurements to the SAFETY Act, and would be well advised to take advantage of the opportunity thus provided whenever and to the maximum extent possible.

One of the more important changes provided by the new Rule is the creation of what are called "Developmental Testing and Evaluation" (DT&E) designations – which can be assigned to any technology (including a service) that is being tested, evaluated, modified, or otherwise being planned for implementation. DT&E designations can be used for only limited periods of time, though – presumptively no more than 36 months; they also can have specific conditions imposed on their applicability, and can be terminated at any time.

An Expedited Review And Other Changes

Many SAFETY Act applicants have been requesting a formalized link between the application review process and the procurements of anti-terror technologies. The new Rule has created such a link, which permits somewhat more creative applications of the SAFETY Act.

Under the new Rule, a government agency (federal, state, or local) can seek a preliminary determination of SAFETY Act applicability through what is called a "Pre-Qualification Designation Notice." That notice will allow a contractor to receive an expedited review and the use of a streamlined SAFETY Act application; in most instances, it also will establish a presumption that the technology under consideration will be a SAFETY Act-approved technology.

The new process will help eliminate the concern that contractors seeking to work in the field of counterterrorism may not receive SAFETY Act approval. This change could be particularly useful for first-responder agencies and organizations that desperately need new cutting-edge technologies but may not have been able to obtain them because of the understandable liability concerns restraining the sellers of the technologies.

The new SAFETY Act Rule includes several other positive changes, including provisions that: (a) make clear that acts of terrorism (including cyber terrorism) occurring on foreign soil may be covered under the SAFETY Act so long as the terrorist act causes at least some harm within the United States; (b) ensure that the term "Qualified Anti-Terrorism Technology" applies to *services* – including design services, software development, threat assessments, vulnerability studies, and program management and integration services – as well as products; and (c) improve the application process by adding changes that make it both simpler and quicker – DHS already has taken steps, in fact, to reduce the review time to 120 days (from the previous 150 days).

Additional changes may be needed in the future, of course, but the initial reaction – from the nation's first-responder agencies and organizations and from the businesses that provide them the systems and services they need – suggests that the changes made possible by the new Rule will result in better use of the SAFETY Act, by more and more companies – and, consequently a better-equipped and more capable first-responder community.

Brian Finch is a Homeland Security Attorney at McKenna Long & Aldridge who focuses his practice on SAFETY Act matters and has already successfully represented many companies in obtaining SAFETY Act coverage. He is also a Senior Fellow at the George Washington University Homeland Security Policy Institute.

Telecommuter Security and the Rules Governing Remote Enemy Access

By Thomas Kellermann, Cyber Security

In 2006, the specters of avian flu and global terrorism loom over the nation's corporate boardrooms. Fear of disease and/or of physical attack has motivated management to depend more heavily than ever before upon Internet-enabled technology. In an effort to preserve business survivability many organizations are providing remote access via wireless technologies to their employees.

The remote-access phenomenon has in fact become a cultural reality in what might be called The Age of the Telecommuter. As demonstrated by the recent Veterans Affairs Administration compromise of 26 million veterans' records, the telecommuter's laptop has become one of the greatest operational risks threatening all networked-intermediated organizations. The 2005 E-crime Watch Survey – produced by the U.S. Secret Service and the U.S. Computer Emergency Response Team – noted that 80 percent of U.S. cybersecurity incidents emanated from outside of the enterprises surveyed.

The dramatic increase in telecommuters has increased cyber risk immensely, with the compromised telecommuter becoming the digital insider. The securing of telecommuter PCs, personal data assistants (PDAs), and other specialized devices has become the most critical of tasks.

Strengthening the Weakest Link

Security is only as strong as the weakest link in the chain, and in the post-9/11 world that chain is becoming increasingly frail. Once a hacker finds the weakest link in a network, he may, through the use of a backdoor Trojan, launch malicious code and vandalize, alter, move, or even delete files. A single compromised computer in a network could lead to the possible contamination of the entire network. Virtual private networks also are at risk of being compromised by hackers. The current *modus operandi* of many hackers is to attack remote computers through wireless systems so they will be able to use the virtual private network as their own.

If the criminal does not exploit the wireless connection, the next easiest way to attack a system is through a "sick" or compromised client computer. Therefore, if security administrators cannot rapidly remediate the vulnerabilities on every computer server and client, all other internal controls may be rendered useless. There is considerable evidence to suggest that the majority of large corporations are over-reliant upon perimeter security. Moreover, because of the vast number of devices involved and the geographical reach of most modern organizations, they find it impossible to maintain real-time situational awareness of the "hygiene/security" of their various technology assets. This reactive stance in the field of security represents a tremendous operational risk.

As business transactions are pushed outside of the traditional enterprise boundaries, critical data is often exposed. A combination of policy, procedure, and technology is required to mitigate if not totally eliminate the risks involved. Today, telecommuter security begins with an *Acceptable Use Policy for Remote Access* that emphasizes the rules of proper cyber-hygiene as well as proper computer use that must be followed. A few examples: Instant messaging should not be allowed. Virus scanners and software patches should be updated on a weekly basis. Laptop hard-drives must be encrypted. And no one should use a specific computer except the person authorized to do so.

Common Sense And Modern Realities

In addition, certain technologies can and should be put to use that can reduce the possibility of the hacker becoming a digital insider. Virtual private networks, two-factor authentication, and encryption are just a few of the tools needed for survival in this amorphous realm.

Even with those and other security tools available there are several specific common-sense rules that should always be followed in securing today's increasingly mobile workforce. Among the most important of those rules are the following: (1) Users should be aware that almost all devices enter and leave a secure network several times a day; (2) once a device is out of compliance with the organization's information-security policy it must be restored quickly; (3) a rogue device may easily become a transit point for numerous hackers and thus can compromise the integrity of the entire network; and (4) telecommuters must remain in compliance with the organization's information-security policy even when they are using non-corporate computers.

To deal with these and other challenging realities, information security officers must acquire technology that can, among other things: (a) authenticate devices before they enter a network; (b) impose a quarantine if and when needed; and (c) subsequently restore a rogue device to a compliant state.

The information-security challenge is likely to become even more complex in the future, for at least two reasons: existing holes in an organization's network security are likely to be kept open by criminal "crews" through the use of backdoor Trojans; and many organizations lack the resources needed to fully determine how compromised their networks have become. In an era of zombied client computers and zero day attacks, it is obviously imperative that senior managers focus their efforts on developing and implementing a layered security program that includes, but is not limited to, proper systems administration and policy management.

Today, the weakest link in the security chain is the telecommuter. In order to preserve the secure enclave in cyberspace, it is crucial not only to recognize the modus operandi of elite hackers but also to ensure, through continuing oversight and policy management, employee compliance with the rules governing the use of all remote devices.

Thomas Kellermann is a cyber security analyst who serves as a member of the Financial Action Taskforce Against Child Pornography and the Anti-Phishing Working Group, and is an active member of the American Bar Association's working group on cybercrime. He is a Certified Information Security Manager (CISM).

Project SeaHawk

Building Unity of Effort in Maritime Security

By Christopher Doane and Joseph DiRenzo III, Coast Guard

"Maritime security is best achieved by blending public and private maritime security activities on a global scale into a comprehensive, integrated effort that addresses all maritime threats." – The National Strategy for Maritime Security

The American "maritime domain" is too vast and the U.S. maritime transportation system too complex for any one government department to secure all of it. During and since the end of World War II, therefore, a broad spectrum of agencies – e.g., the U.S. Customs Service, the U.S. Coast Guard and U.S. Navy, various state port authorities, local police departments, shipping companies, and port terminal operators – have conducted their own maritime-security operations. These agencies frequently, but not always, have loosely coordinated their activities with one another, and on some occasions have conducted joint operations, particularly when a criminal threat overlapped their respective jurisdictions.

> **Project SeaHawk "has created a unified intelligence operations center that includes all federal, state, and local agencies having responsibility for any aspect of port security and protection."**

Usually, though, they have operated independently, focusing on their own specific concerns and within their own jurisdictions. Following the terrorist attacks of 11 September 2001, however, and the belated recognition of how vulnerable the overall U.S. transportation system is to international terrorism, the need for federal, state, and local security agencies as well as the private sector to unify their efforts to protect the nation's maritime assets became a cornerstone concept of the U.S. security strategy.

Recognizing the need for unified maritime security is one thing; making it a reality is a different – and much more difficult – matter. Through the Maritime Transportation Security Act of 2002, the U.S. Congress designated Coast Guard Captains of the Ports (COTPs) as the federal maritime security authorities responsible for coordinating security in the ports to which they were assigned.

Creating Combined Communications Capabilities

The Act also required – and the COTPs have established – the creation of area maritime security committees consisting of federal, state, local, and private-sector members. Creation of the committees already has improved communication among the members and led to the development of joint plans to enhance coordination for the security of U.S. seaports. There remained, though, an equally important need – namely, the coordination of day-to-day security operations within the port area.

As a first step toward meeting this need, the Coast Guard and Navy formed a Joint Harbor Operations Center – in Norfolk, Va. – where Coast Guard and Navy watch standers monitor activities throughout the port and coordinate the response of field security units to investigate unusual or suspicious activity. A similar center is now operational in San Diego, and more are planned for other U.S. ports where the Navy and Coast Guard both have a significant presence.

Although a helpful first step, the Norfolk and San Diego centers involve only two agencies. A more comprehensive effort, involving a larger number of maritime stakeholders, obviously is necessary – and that need also is being addressed. One such effort that has received considerable attention in recent months has been the Charleston Harbor Operations Center, commonly known as Project SeaHawk, in Charleston, S.C.

The second largest container port on the U.S. east coast and the fourth largest container port in the United States, Charleston processes the equivalent of over 1.5 million twenty-foot containers annually, according to data compiled by the Charleston Southern University Center for Economic Forecasting. Such a massive volume of maritime commerce obviously provides numerous opportunities for exploitation by criminal or terrorist groups. To address that problem, and reduce U.S. maritime vulnerability in general, then-U.S. Senator Fritz Hollings (D-S.C.) sponsored the bill that created and funded the SeaHawk program.

A Broad Spectrum Of Meaningful Opportunities

Formed and directed by the U.S. Attorney's Office for the District of South Carolina, Project SeaHawk, which is sponsored by the Department of Justice (DOJ), operates out of a new high-tech facility staffed with officers from a broad spectrum of agencies, from all levels of government, that have been assigned varying degrees of maritime responsibilities – the U.S. Customs and Border Patrol, for example; the Coast Guard and Navy; the FBI; Immigration and Customs Enforcement; and, last but by no means least, local police departments and several state law-enforcement agencies.

SeaHawk watch standers continuously monitor surveillance video and analyze data from dozens of sources to develop meaningful risk assessments of cargo movements of all types. Following those assessments, task force members with the operational skills needed are assigned, as and when necessary, to board vessels, inspect cargo, and/or conduct harbor patrols – a clear and positive demonstration of unity of effort in action.

Perhaps the greatest value of the center is the opportunity it gives officers from all of the agencies participating to rapidly come together to plan joint responses to any perceived threat. That value was confirmed by the National Law Enforcement and Corrections Technology Center's Justice Technology Information Network (JUSTNET), which noted that Project SeaHawk "has created a unified intelligence operations center that includes all federal, state, and local agencies having responsibility for any aspect of port security and protection.

"A combined task force will address all areas of security to include screening ship crews, itineraries, and manifests, as well as the physical aspects of daily port operations," the JUSTNET analysis also noted. "The goal is [creation of] an operational task force that will evolve systematically into a model that can be easily replicated at other ports throughout the nation."

Plaudits From Allen, DeMint

The idea that SeaHawk may well serve as a model for additional, and perhaps even more ambitious, joint command-and-control (C2) efforts was reinforced last month by Coast Guard Commandant Admiral Thad Allen, who pointed out – in an interview with *DPJ* Managing Editor John Morton – that SeaHawk is "one of three or four business models" for additional (local) C2 efforts within U.S. ports. Another example, of course, is the Joint Harbor Operations Command described earlier. The C2 models were developed, Allen continued, "in response to local requirements." The SeaHawk Project, he noted, "evolved from the Joint Terrorism Task Force [JTTF] with the U.S. Attorney … [and has] a justice focus."

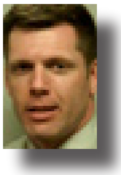
The SeaHawk Project received additional high-level attention earlier this month when Senator Jim DeMint (R-S.C.) toured the Charleston center on the 11th of August. "Project Seahawk is on the cutting edge of port security," DeMint said following his visit, "and it's something we need around the country." A member of the Senate's Commerce, Science, and Transportation Committee, DeMint said he already has asked Committee Chairman Ted Stevens (R-Alaska) to "make sure we begin taking steps to use this program nationwide." Stevens "told me," DeMint said, that "he would add it to the port- security bill, so I'm confident we are one step closer to making this bill a reality."

The fact that Project SeaHawk is already considered to be a model of how multiple agencies can be brought together to leverage their respective expertise and capabilities to provide comprehensive port security is perhaps the best evidence of how successful the project has been. The suggestion that senior officials are considering how to translate the SeaHawk concept to other ports is further evidence, and illustrates the importance of the multi-agency cooperation emphasized in the National Strategy for Maritime Security.

Christopher Doane (pictured on previous page) and Joseph DiRenzo III are retired Coast Guard officers now serving as Coast Guard civilian employees; both also are Visiting Fellows at the Joint Forces Staff College. Although management experts in and out of government were consulted in the preparation of this article, the opinions expressed in the article are their own.

Missouri, Hawaii, Rhode Island, Louisiana, Oregon, and California

By Adam McLaughlin, State Homeland News



Missouri
Canine Teams Help Lambert Field Airport Upgrade Cargo Security

Thanks to the addition of eight canine teams, Lambert Field airport, located in St. Louis, is now one of only a few of the nation's airports able to screen every piece of cargo that boards a passenger plane. Last April, Lambert Field Police Chief Paul Mason made the decision to have the airport's canine teams spend more time screening cargo and watching cargo areas.

"Using canines to close screening gaps at Lambert has not sacrificed the security presence elsewhere, such as terminals and airport parking garages, but instead requires better management and paying some overtime," Mason said. "We are happy with what our canine teams have been able to accomplish," he added at a news conference inside the Southwest Airlines cargo facility.

The dogs are taken through the airport's airline cargo facilities early each morning to check all unscreened boxes. The canine teams carry out additional screening throughout the day, then conduct a final sweep when the cargo holds close. The Transportation Security Agency (TSA) reimburses the airport $50,000 a year for each bomb-sniffing dog, about 60 percent of what the airport spends on the dogs and their handlers.

TSA does not require airport security to screen all cargo carried on passenger flights. In November 2005, the Government Accountability Office reported that approximately two billion pounds of cargo shipped by air each month is barely checked. TSA does require, though, that all cargo shipped on passenger flights must be handled by companies that meet TSA's cargo-safety guidelines. This spring, TSA started to require background checks of over 50,000 off-airport freight-forwarder employees.

> *The canine teams carry out additional screening throughout the day, then conduct a final sweep when the cargo holds close*

Hawaii
Honolulu Upgrade's Its Radio Communications Towers

Honolulu officials have announced that eight of the city's 24 radio communications towers are being replaced as part of a $22 million project to update the network that emergency responders rely on each day. The towers serve as a critical link in the city's communications network, enabling police, fire, and emergency medical services personnel to communicate with one another and within their respective departments.

Gordon Bruce, the city's information technology director, said that workers already have begun replacing the towers, which continue to operate despite their rusted and worn condition, on a schedule of two to three new towers a year. After it was reported that some of the metal towers were deteriorating, Honolulu Mayor Mufi Hannemann told Bruce to make the communications update one of his top priorities. Bruce estimated that the eight towers in the greatest need of repair will be replaced within three years, and that another five will be repaired or replaced by 2009.

The new structures will be built to withstand a Category 4 hurricane, city officials said. If some towers are disabled, the signals can bounce to and between other towers to bypass the problem area. A fiber-optic system will provide emergency backup capability.

Rhode Island
National Guard CST Makes Official Debut

The 13th Weapons of Mass Destruction (WMD) Civil Support Team (CST), based in Coventry, is now ready for rapid deployment to support local, state, and federal authorities in responding to any attack involving chemical, biological, radiological, or explosive munitions.

The 22-member, full-time National Guard unit earned national certification last month following nearly three years of training. "The team worked very hard to develop the skills to be 100-percent proficient to respond to a WMD incident," said Rhode Island Adjutant General Lt. Col. Robert T. Bray. "If an incident were to take place, the local emergency responders would conduct an initial assessment," he said, "[and] then could make a direct request for assistance from our Civil Support unit."

Certification of the 13th WMD CST makes it one of the 40 teams around the country that have received national certification since the program was launched eight years ago. The team is federally funded through the National Guard Bureau. The first year is expected to cost approximately $7 million to establish a team and purchase equipment. That estimate does not including training costs and salaries for the full-time Guardsmen.

"Most of the team's soldiers, men and women, are from Rhode Island, which helps," said Lt. Col Paul R. Peltier, the unit's commander. "They know the area and are familiar with the community. Their families live here, so you get the extra dedication," he said.

The initial priorities of the team members are to educate themselves through research on various chemical and biological agents such as anthrax – the goal is not only to understand what those agents are, but also how to recognize them when they are described by a local authority. The team also plans to conduct a series of exercises with local emergency responders, such as firefighters and policemen.

> ***Some structures built in accordance with the latest codes would tumble and the damage would be even more extensive for buildings constructed to laxer standards***

Louisiana
Hurricane Season Goal: 150,000 Shelter Beds

Louisiana emergency-management officials reached agreement with the federal government last week to try to have 150,000 shelter beds ready for use within the state during and in the aftermath of future hurricanes that require major evacuations. There are now approximately 90,000 beds available.

Federal officials have emphasized that they cannot ask other states to provide shelters if Louisiana does not provide maximum assistance to its own residents. However, the state's senior emergency-preparedness official, Col. Perry Smith Jr., expressed skepticism that there is currently enough capacity in Louisiana to reach the target goal of 150,000 beds set by the federal government.

Gil H. Jamieson, the principal Department of Homeland Security (DHS) official in Louisiana, said earlier in the week that all of the agencies involved are now working from the same lists and trying to reach the same bed threshold. In addition, the Federal Emergency Management Agency (FEMA) has agreed to help obtain the personnel needed to open the shelters. Louisiana officials had emphasized that finding staff would be the key to expanding the number of shelter beds available. "From a facility standpoint, we have got it," Jamieson said. "The issue right at the moment is not the [shelter] facilities, but access, provisioning, and securing of the facilities.

"The federal government will get enough staff ready to run the shelters," he added, "by working with the American Red Cross and other volunteer groups." It is generally agreed that providing shelter for people with no place to go is one of the most critical aspects of preparing for coastal evacuations. An estimated 40,000 evacuees ended up in shelters outside Louisiana in the aftermath of Hurricane Katrina.

Oregon
Civil Air Patrol Conducts Seismic Survey Exercise

The Oregon Wing of the Civil Air Patrol (CAP), working in cooperation with the United States Geological Survey (USGS), will be participating in a six-state seismic-survey event this weekend (August 25-27). The survey exercise will be part of a national program to better understand local seismic danger spots and to practice emergency-response procedures that would be used following a major seismic event in the Pacific Northwest.

The Oregon CAP wing will use its new Satellite Digital Imaging System to provide aerial photography capabilities during the exercise, officials said; the images will involve "points of real interest," the officials said, and the photos taken will be used for future USGS research. The Oregon CAP will be operating out of the Willamette Aviation Service located at the Aurora State Airport; an estimated seven aircraft and fifty personnel will be participating in the event.

One reason for the exercise, as USGS officials pointed out, is that volcanoes are not randomly distributed over the surface of the earth. In fact, more than half of the world's active volcanoes above sea level encircle the Pacific Ocean to form the circum-Pacific "Ring of Fire." There are more than 500 "active" volcanoes – i.e., those that are known to have erupted at least once within recorded history – in the world, and 50 of the 500 are in Oregon, California, Washington, and Hawaii.

California
University Develops 3-D Earthquake-Simulation Software

In early August, structural engineers from the California Institute of Technology (Caltech) used supercomputer simulation models to determine what might happen if a massive earthquake affected tall buildings in the Los Angeles area. The results, according to the researchers, provide both a hint at the possible devastation that might be caused by the next real earthquake in the area, and a starting point to build future generations of even more accurate models. The research is believed to have been the first to combine detailed earthquake and building models in a single three-dimensional simulation.

One of the hypothetical earthquakes, a magnitude 7.9, started in Parkfield and spread down the San Andreas Fault, leaving a 180-mile scar in the earth and shaking communities in the San Fernando Valley. Through use of the supercomputer, the engineers were able to watch as the shifting earth jostled imaginary 18-story buildings throughout the Los Angeles area. Many of those buildings would not survive, according to the test results. Some structures built in accordance with the latest codes would tumble, in fact, and the damage would be even more extensive for buildings constructed to laxer standards. Some of the office structures in Santa Monica, West Los Angeles, and the areas around Baldwin Park, Compton, and Seal Beach, toppled completely.

"If you look very carefully at the ground motions that come out of their new methodology, they are significantly larger than the ground motions we would normally put into building design and analysis," said William Iwan, a Caltech earthquake engineer. "If this [the results of the supercomputer simulation] really is true and verified, it means that building engineers need to go back and look [again] at building design."

Adam McLaughlin is Preparedness Manager of Training and Exercises, Operations, and Emergency Management for the Port Authority of N.Y. & N.J. He develops and implements agency-wide emergency response and recovery plans, business continuity plans, and training and exercise programs. He is a former U.S. Army Military Intelligence & Security Officer.