



# Counter-Terrorism Protecting the Homeland

**Privatizing War**

**PMCs: The Invisible Force Multiplier**

Dr. Neil Livingstone  
GlobalOptions, Page 5

**Chemical Nerve Agents: A 24/7 Threat**

Jerome Hauer  
Viewpoint, Page 7

**The Need for Intelligence-Led Policing**

Michael Barrett  
Law Enforcement, Page 8

**Brigadier General Simon Perry  
Israel National Police**

John Morton  
Podcast, Page 6

**The IED Problem: Solutions  
On Display, And On the Way**

Robert Besal  
Viewpoint, Page 18

**Terrorism: The Cyberspace  
Battleground**

Thomas Kellermann  
Cyber Security, Page 11

**The JTTFs -  
"Jointness" at Its Most Effective!**

Christopher Doane, Joseph DiRenzo III,  
and Jeffrey Robertson  
Coast Guard, Page 14

**Toronto & the U.S. Canadian Border:  
What Should And Should Not  
Happen Next**

Joseph DiRenzo III and Christopher Doane  
Viewpoint, Page 16

**Louisiana, Alabama, Washington DC,  
Missouri, Mississippi, and Texas**

Adam McLaughlin  
State Homeland News, Page 9



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



**Arriving first on the scene means you never know what you're going to encounter.**

Today that could include life-threatening chemical nerve agents which may be lethal in seconds.



Immediate evacuation and wearing PPE is essential, as is being equipped with auto-injectors that are designed to administer antidotes in emergency situa-

tions such as these. Unlike a syringe which can be cumbersome and time-consuming, auto-injectors provide a quick and portable drug delivery in just two steps.

**Hope for the best.  
Prepare for the worst.**

You can't rely solely on antidotes for protection, but you can be better prepared for the worst. Call today—Meridian can help you prepare.

**MERIDIAN**  
MEDICAL TECHNOLOGIES™

Protecting Those who Protect Us™

[www.meridianmeds.com](http://www.meridianmeds.com)  
**800.638.8093**

©2006 Meridian Medical Technologies™, Inc.,  
a subsidiary of King Pharmaceuticals® Inc.  
PN: 5-1084-1

## PUBLISHER'S MESSAGE

By Martin (Marty) Masiuk



When the ragtag militias, pirates, and untrained civilian volunteers led by Andrew Jackson and Jean Lafitte won their decisive victory over the British in the 8 January 1815 Battle of New Orleans, few if any Americans then living dared to dream that it would be the last time, for almost two centuries, that U.S. citizens would be called on to protect their own homeland from foreign attack.

The days of dreaming are now over, though, and have given way to the recognition of several harsh realities, the most important of which is that in the Age of Terrorism no American citizen is, or should feel, truly safe anywhere in the world.


The United States is today, by any standard of measurement, the most powerful nation in history – politically, economically, and militarily. For that reason alone, the U.S. homeland and the American people are and will continue to be – for psychological and propaganda reasons as well as political purposes – the principal targets of the international terrorists who for their own warped reasons hate and seek to destroy Western culture, Western values, and, ultimately, Western civilization itself.

As has happened too many times throughout this nation's history, the American people, and their elected leaders, dithered and delayed far too long before facing up to the clear and present – and unprecedented – danger that now threatens not only their own lives, and their children's, but also the U.S. homeland itself. The tide of public opinion seems gradually to have turned, fortunately, and there is clear evidence, as spelled out in several articles in this issue of *DomPrep Journal*, that progress in this twilight war is being made not only overseas but on the U.S. home front as well.

Not surprisingly, the U.S. private sector has contributed significantly to that progress, as Neil Livingstone points out in his lead article on the increasingly important (but little-recognized) role played in Iraq by the PMCs (private military companies) that have so capably augmented the combat efforts of the active forces.

The IED 2006 Symposium and Expo in Fayetteville, N.C., earlier this month provides an excellent example of how U.S. armed forces are working with private industry to counter the IED (improvised explosive device) threat that already has caused more than 16,000 casualties in Iraq and Afghanistan. Rear Adm. Robert Besal, USN (Ret.), a new contributor, provides *DPJ* readers an exclusive report on that conference.

Other hopeful signs of progress spelled out in this issue are the apprehension in Toronto of the 17 terrorists allegedly planning to assassinate Canadian political leaders and to attack key infrastructure targets; the increasingly closer cooperation between the United States and Israel in their efforts against the common enemy of both nations; the initiatives taken by several states to improve local preparedness plans and capabilities; and the persuasive rationale for adoption of intelligence-led-policing policies and programs to help counter domestic terrorism. (These articles are balanced by others spelling out the still not fully realized dangers posed by cybercrime terrorists, and by chemical nerve-agent weapons and devices.)

As always, your comments and critiques about this issue are hereby solicited, and will be much appreciated. 

*About the Cover:* U.S. Army Soldiers engage simulated insurgents during combat operations training in the mock city of Al Jaff at the national training center on Fort Irwin, Calif., May 2, 2006. The Soldiers are from 2nd Battalion, 27th Infantry, 3rd Infantry Combat Brigade Team, 25th Infantry Division. (U.S. Army photo by Master Sgt. Johancharles Van Boers)

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

**Staff**  
Martin Masiuk  
Publisher  
mmasuk@domprep.com

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

John Morton  
Managing Editor & Interviews  
jmorton@domprep.com

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

Sharon Stovall  
Web Content Research  
sstovall@domprep.com

Paige Dunn  
Advertising Sales Coordinator  
pdunn@domprep.com

### Advertisers in this Issue:

- Canberra, Inc.
- EJ Krause and Associates
- Meridian Medical Technologies, Inc.
- RAE Systems

© Copyright 2006, by IMR Group, Inc.; reproduction of any part of this publication without express written permission is strictly prohibited.

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

Articles are written by professional practitioners in homeland security, 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.





# Your One Source for Radiological Incident Response

In the event of a radiological terror attack or radiation accident, emergency responders need the very best tools.

With the CANBERRA UltraRadiac first responders get fast responding, ultra rugged radiation monitoring. The large display is easy to read — even through masks — and audible, visual and vibrating alarms ensure the first responder always knows the hazard level at his/her own location.

As the situation unfolds, emergency responders need to control and contain contamination. Deploy a MiniSentry Transportable Portal Monitor in less than 10 minutes to begin screening victims, responders, and the public — keeping contaminated material from leaving the scene. Then use ergonomically designed Radiagem survey kits and InSpector 1000 radiation identifiers to quickly locate and identify contamination for removal — minimizing the radiation exposure of both victims and responders.

#### Best equipment solves only part of the problem.

CANBERRA also offers training courses designed specifically for the first responder — free of technical jargon and focused on the practical aspects of first response to incidents and attacks.

#### Prepare now!

Call CANBERRA today or visit our web site!

[www.canberra-hs.com](http://www.canberra-hs.com)

Canberra Industries, Inc.  
800 Research Parkway – Meriden, CT 06450 U.S.A.  
Tel: (203) 238-2351 – Toll free: 1-800-243-4422  
Fax: (203) 235-1347

**A**  
**CANBERRA**



UltraRadiac Personal  
Radiation Monitor

Radiagem Kit for  
surveying



InSpector 1000 for  
source location  
and nuclide  
identification



MiniSentry  
Transportable  
Portal Monitor

**DomPrep Channel Masters****First Responders:**

Rob Schnepf  
Fire/HAZMAT  
rschnepf@domprep.com

Chris Hawley  
Fire/HAZMAT  
chawley@domprep.com

Brian Geraci  
Fire/HAZMAT  
bgeraci@domprep.com

Joseph Cahill  
EMS  
jcahill@domprep.com

Michael Barrett  
Law Enforcement  
mbarrett@domprep.com

**Updates:**

Adam McLaughlin  
State Homeland News  
amclaughlin@domprep.com

**Borders & Ports:**

James Hull  
Coast Guard  
jhull@domprep.com

Joseph DiRenzo III  
Coast Guard  
jdirenzo@domprep.com

Christopher Doane  
Coast Guard  
cdoane@domprep.com

Luke Ritter  
Transportation Analysis  
lritter@domprep.com

**Military Support:**

Chris Schnaubelt  
Homeland Defense/NorthCom  
cschnaubelt@domprep.com

Jon Dodson  
National Guard  
jdodson@domprep.com

**Commentary:**

Neil Livingstone  
GlobalOptions  
nlivingstone@domprep.com

**Medical Support:**

Jerry Mothershead  
Military Medicine  
jmothershead@domprep.com

Michael Allswede  
Hospital Administration  
mallswede@domprep.com

Duane Caneva  
Public Health  
dcaneva@domprep.com

**Funding & Regulations:**

Brian Finch  
Safety Act  
bfinch@domprep.com

Mary Ungar  
Funding Strategies  
mungar@domprep.com

Thomas Kellermann  
Cyber Security  
tkellerman@domprep.com

**Privatizing War*****PMCs: The Invisible Force Multiplier***

By Dr. Neil Livingstone, GlobalOptions



One of the most dramatic changes in the U.S. military establishment over the past quarter century has been the explosive growth of outsourcing to private contractors of an increasing number of functions that were traditionally performed by military forces. Those functions include almost everything from the preparation of meals to trash collection, the building and maintenance of camps and bases, equipment maintenance, the interrogation of prisoners, recruiting new enlistees, driving trucks and flying helicopters, and even guard duty. Companies like Halliburton are reaping vast sums of money by providing support services to the Pentagon. According to one senior Pentagon official, the U.S. military would collapse without this support.

Until recent years, however, contractors were limited to support functions and not to actual combat roles. But that is changing, and a new breed of business, known as the private military company (PMC), is emerging. Today, in Iraq alone, there are anywhere from 50,000 to 100,000 contract employees, as many as a quarter of them providing security services – which, on occasion, involve actual combat with the enemy. According to Peter Singer of the Brookings Institution, the firms providing security services in Iraq “have sent more troops and taken more casualties than all of our other reluctant allies combined.”

Many of those who work for the PMCs are former special operations veterans who retire from the military and then ply their skills in the private sector for considerably more money. Among the better known PMCs operating in Iraq are MPRI (Military Professional Resources Inc.), Olive Group, AEGIS Specialist Risk Management, Control Risks, Triple Canopy Inc., and Blackwater USA.

***Budget Realities and Legal Issues***

But, although Iraq has certainly spurred the growth of PMCs, it is by no means the only market for such companies, which today are operating throughout the world. PMCs are protecting oil fields and pipelines, guarding airports and seaports, securing vessels on the high seas, protecting mining concessions,

guarding celebrities and VIPs, ferreting out intellectual property theft and the counterfeiting of branded products, and even protecting endangered species from poachers.

The growth of PMCs has mirrored the expansion of the security industry on a domestic basis. Throughout the United States, law-enforcement budgets have been stretched to the limit and, were it not for the millions of private security guards and cameras, crime might well be out of control. Indeed, private security cameras often provide crucial evidence in criminal cases, such as the 1995 Oklahoma City bombing.

Today, some PMCs have larger and more formidable military capabilities than many of the world's smaller countries. This raises the question of the legal status of such companies in the modern world. Critics of PMCs say that they often cross the line and are, in effect, mercenary organizations. Among the best known mercenary companies in recent years were Executive Outcomes, which operated throughout Africa in the 1990s; Sandline International, which closed in April 2004; and Gurkha Security Guards Ltd., which was active in the Sierra Leone civil war. A number of other firms also provide men for the Praetorian Guard units of various developing countries, especially in Africa.

***Mercenaries? Or Civilian Contractors?***

In December 1989, the United Nations promulgated the International Convention Against the Recruitment, Use, Financing, and Training of Mercenaries. The Convention entered into force on October 20, 2001, less than six weeks after the terrorist attacks on the World Trade Center and the Pentagon. It is worth noting that, despite the United Nations' opposition to such companies, the PMCs have, on occasion, performed contract work for the world body.

But what is the distinction between a mercenary and a military contractor? In the 1977 Protocol Additional to the Geneva Conventions of August 12, 1949, a mercenary is defined as “any person who is specially recruited locally or abroad in order to fight in an armed conflict,” who takes “a direct part in hostilities,” “is motivated to take



part in the hostilities essentially by the desire for private gain," and "is neither a national or a Party to the conflict nor a resident of territory controlled by a Party to the conflict." That definition would seem to include many employees of today's PMCs.

Traditionally, civilian contractors did not directly participate in hostilities, but that also has changed, especially in Iraq and Afghanistan. The U.S. government argues that companies like Blackwater USA do not fall under the mercenary provisions of international conventions because they are supporting the armed forces of a party to the conflict – i.e. the United States.

### Other Markets Also Available

Private contractors also are part of the intelligence-collection process, both for government agencies and private-sector clients. Some of these companies are PMCs; others could best be classified as private intelligence companies (PICs), because they do not provide military support services.

Just as the Pentagon is short of manpower and resources, so too is the CIA. The CIA's Directorate of Operations (DO) has recruited private companies and individuals to handle what once were exclusively in-house functions, including the raising and support of paramilitary forces, the interrogation of prisoners, the filling of transportation requirements, and even some covert operations.

Many companies provide multinational corporations with competitive intelligence and facilitate entry into difficult markets, where it may be necessary to deal with warlords, mafia chieftains, and political instability. It also is not unusual for private companies to investigate industrial espionage and intellectual property (IP) theft. In some cases, such companies conduct quiet wars against IP pirates and their government allies. That task is particularly important in countries like China, where the government does little either to protect foreign intellectual property or to enforce its own laws concerning piracy and other violations of trademarks, patents, copyrights, contracts, service marks, and the theft of trade secrets.

### The New Feudalism

A quarter of a century ago, Robert A. Nathan, writing in *Foreign Policy*, warned that an increasing number of companies were engaged in the usurpation of police and military powers, and that some of their activities amounted to little more than a "return to the wild west." According to Nathan, "If the international corporate sector seeks protection by private counter-terrorist security firms, a medieval situation may emerge in which the security function of the state is usurped by private contractors." He described this emerging situation as "the new feudalism."

It is doubtful that even Nathan could have imagined the size and number of private military companies operating today. As long

as military resources are strained across the globe, there will be plenty of work for private contractors. And the scope of their activities can only be expected to increase in the years ahead.

Such activities are not inconsistent with the U.S. Constitution. Indeed, the founding fathers expressly anticipated a role for the private sector in the defense of the nation. The Constitution gives Congress only three war-making powers: declaring war, raising armies, and the issuance of Letters of Marque and Reprisal. Letters of Marque and Reprisal are essentially grants by Congress to private individuals to carry out military actions against enemies of the United States – historically, this usually meant maritime pirates.

Just as private individuals, bearing Letters of Marque and Reprisal, played an important role in ending piracy on the high seas (some still exists, but in relatively isolated areas), in the world of the 21st century it should not be surprising that private contractors are and will be crucial to winning the war against terrorism.

---

*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.*

## LEARN FROM WORLD-CLASS AUTHORITIES - WITHOUT LEAVING YOUR DESK!



### Upcoming Audio Interviews

**Brigadier, General Simon Perry, Israeli National Police**

**Admiral Thad W. Allen, USCG, Commandant, U.S. Coast Guard**

**George W. Foresman, Under Secretary for Preparedness, DHS**

DomPrep Journal Managing Editor John Morton conducts one-on-one question-and-answer sessions with senior preparedness professionals. Solutions, policies, and other authoritative information is delivered to you in easy-to-listen interviews without you having to leave your desk.

**\*FREE With Registration**

Visit [www.DomesticPreparedness.com](http://www.DomesticPreparedness.com) for more details



# Chemical Nerve Agents: A 24/7 Threat

By Jerome Hauer, Viewpoint



For five seasons of Fox's hit television show "24," lead character Jack Bauer and his colleagues at the Counter Terrorism Unit have struggled to protect the United States from threats ranging from bio-terrorism to nuclear attack. This makes for great entertainment, but it also reflects the real threats that the American people and their Free World allies now face every day.

The plotline for this season's "24" has focused largely on a terrorist threat involving a chemical nerve agent. Although not considered as high-impact as a nuclear device or biological agent, a chemical nerve agent is a much more probable weapon of choice for the practical terrorist.

Unlike nuclear or biological weapons, chemical nerve agents are relatively easy and inexpensive to produce and deploy. These poisons – which include organophosphorous insecticides such as malathion, parathion, and diazinon – are readily available in many communities throughout the country, and travel via road and rail through American cities every day.

Chemical nerve agents already have been used successfully in terrorist attacks. In 1995, members of the Japanese cult Aum Shinrikyo released the nerve agent sarin into a Tokyo subway, killing 12 people and poisoning 5,500 others. The year before, members of the same cult released sarin into a residential apartment building in Matsumoto, Japan, killing seven and poisoning more than 200.

## Two Shortages: Time, and Antidotes

"Planning Scenarios," a report issued by the Homeland Security Council in July 2004, outlined a terrorist attack scenario in which a chemical nerve agent released in three large office buildings could kill 95 percent of the occupants – i.e., nearly 6,000 people. The report estimated that first responders would arrive on the scene in 10-15 minutes. But that seemingly fast response would likely be too little and too late, given the rapidity of onset of nerve-agent poisoning symptoms and the

extremely difficult if not impossible logistical challenge of providing immediate medical assistance to large numbers of victims.

In the event of a chemical nerve agent attack on a public transit system, indoor stadium, amusement park, or office building, those who have been poisoned may have only minutes to receive the antidote. Emergency responders in the United States have access to auto-injectors that contain the antidotes for chemical nerve agent poisoning. The problem is that, in many cities, the emergency responders may have only enough antidotes to treat themselves, and would not be able to treat victims in time.

Hurricane Katrina underscored the fact that local emergency responders must be prepared to manage a disaster for a period of 24 to 72 hours before federal assistance arrives. Unfortunately, most state and local emergency-management agencies do not have a standardized protocol to guide their response to a chemical nerve agent attack. Most are depending on having access to federal government stockpiles of antidotes, which are stored in strategic holding sites throughout the country. But those caches would not be immediately available, if only because it would be logistically impossible to transfer the antidotes from the holding sites to the attack sites in the short amount of time required for the antidote to take effect. Moreover, most of the antidote stockpiles do not have adequate supplies of infant and pediatric dosages.

## NYC Sets the Example

Even before the 9/11 terrorist attacks, New York City implemented a layered inventory and response system designed to meet the nerve-agent challenge. Every ambulance in the city now carries an inventory of chemical nerve agent antidote kits as standard equipment. The victims who are most severely affected by a nerve agent would receive their initial antidote treatment from the first ambulances to arrive on the scene.

Logistical Support Units – specialized teams that ensure responders have the supplies they need – represent the next layer of logistical support, with pre-positioned caches of

*Not as high-impact as a nuclear device or biological agent, a chemical nerve agent is a more probable weapon of choice for the practical terrorist.*

antidotes serving as the third layer. These local layers of reinforcement would be used before federal assets, such as the chem-packs supplied by the Centers for Disease Control and Prevention, would be required. For planning purposes it is obviously of vital importance, in the event of an emergency, that local first responders have immediate access to the antidotes.

State and local emergency-response agencies now have the opportunity to purchase chemical nerve agent antidote kits through federal Office of Domestic Preparedness grants, at no cost to the state or local community. This change gives emergency-planning and response-agency leaders the opportunity to partner, *in advance*, with other state and local government officials to assess the risk of a chemical nerve-agent emergency occurring in their home communities, and to develop standard response protocols similar to those now in place in New York City.

During an emergency is not the time to realize that local responders do *not* have a plan in place. And Hollywood heroes such as "24's" Jack Bauer will not be there to save the day.

For more information on first-responder grants, visit the Department of Homeland Security Web site at [www.dhs.gov/dhspublic/interapp/editorial/editorial\\_0356.xml](http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0356.xml).

Jerome Hauer is former director of the New York City Office of Emergency Management and former assistant secretary, Department of Health and Human Services, Office of Public Health Emergency Preparedness.

# The Need for Intelligence-Led Policing

By Michael Barrett, Law Enforcement



Recent decades have witnessed a rapid spread of communications and other technologies across all facets of society, enabling small and previously disparate groups to better coordinate their activities and learn from one another in furtherance of their common objectives. These advances have of course increased the productivity of the U.S. population at large, but at the same time have created new opportunities for those outside the law, including organized criminal elements and terrorists.

One result of these societal changes is that today's criminals are displaying increased sophistication and operational agility in their efforts to subvert law and order, and that in turn has created a need for U.S. law-enforcement agencies – local, state, and federal – to concentrate their collective law-enforcement efforts in a more structured manner and to modernize the various business processes they use to determine resource allocations. Experience suggests that the optimum way to achieve these goals is through a new series of processes and procedures that form the structural components of what is called Intelligence-Led Policing (ILP).

Intelligence-led policing is a management philosophy developed in the United Kingdom to ensure that resource allocations are based primarily on an improved awareness of the operating environment. It also is a collaborative philosophy that supports decision makers, through data collection and intelligence analysis, to improve their situational awareness and thus enable them to optimize their crime-control strategies, the allocation of resources, and tactical operations guidelines.

## The Key Requirements

The adoption of ILP processes requires a concerted effort by all parties – including analysts, operators, and senior leaders – involved in planning and/or operations. For analysts, the key components of the ILP processes include the creation of tactical, operational, and strategic intelligence products that support immediate needs, promote situational awareness, and provide

the foundation for longer-term planning. For operators, ILP requires that they become not only better data collectors but also better consumers of intelligence-related products – shifting, if and when required, from emphasizing post-event evidence collection to gathering data for entry into appropriate databases and, later, drawing from the databases and intelligence analysts the information needed to support ongoing operations.

For senior leaders, the decision to adopt an ILP philosophy requires them to work more closely with both analysts and operators to ensure that a common and accurate operational picture is driving the distribution of resources.

## Data + Analysis = Intelligence

Intelligence-led policing often requires a structural reorganization that not only supports data collection but also the creation, dissemination, and cataloguing of intelligence products to drive strategic decision-making and a structured allocation of resources. It also defines the processes associated with intelligence that will be incorporated into crime-prevention strategies. The primary aspect of this process is bounded by the five interlocking processes of what is called the Intelligence Cycle: Planning and Direction; Collection; Processing and Collation; Analysis and Production; and Dissemination and Integration.

## Data vs. Intelligence

In this context, intelligence can be defined as the synthesis of known data and analytical reasoning to create a reasonable determination about the overall operating environment. Unfortunately, the term *intelligence* is often but incorrectly used interchangeably with two rather different terms: *data*, and *information*. In the past, some very difficult problems have been created when law-enforcement agents have misused official intelligence and/or when the general public has misunderstood the nature of the data being collected. For that reason alone it is particularly important that special care be taken when describing the nature of the information in question.

“Data” refers simply to raw information that has been collected but has not yet been analyzed. Nonetheless, in most operational situations it is vitally important, for two reasons, that a large and varied amount of data be collected: First, data is often perishable in nature and may be lost forever if it is not collected and catalogued at the earliest opportunity. Second, seemingly innocuous data might quickly become critical information as a result of post-collection analysis. This is, in fact, why all evidence at a crime scene should be carefully catalogued: in case it later becomes relevant to the case.

In short, therefore, intelligence is the product of careful evaluation and analysis of all of the data collected. That product is then disseminated in reports and other ways to help operators, analysts, and senior leaders better understand their collective operating environment and to drive the appropriate allocation of resources.

The adoption and implementation of an ILP policy and organizational philosophy will require the U.S. law-enforcement community to adjust its operational processes to bring improved structure to its near-, mid-, and long-term planning cycles while at the same time optimizing its resource-allocation decisions. To facilitate these several changes will require a concerted effort by all parties involved – analysts, operators, and senior leaders – to ensure that the end result is an appropriate variant of the ILP model that is consistent with the agency's mission, strategy, and core values.

## Guidelines, Tenets, & Components

As guidelines, it would help to remember the three principal tenets of the ILP process: ensure an adaptable force construct for flexible deployment; follow the Intelligence Cycle for the analysis of data; and use intelligence-driven analyses to set priorities and allocate resources.

For analysts the key components of the ILP process include the creation of tactical, operational, and strategic intelligence products that support immediate needs, promote situational awareness, and provide the foundation for longer-term planning. The intelligence analyst also plays a particularly important role in the



Intelligence Cycle. In addition to assisting in the creation of the collection intent, the intelligence officer is responsible for ensuring that the agency's collection plan remains a dynamic, living product.

For operators the ILP process requires becoming better both in the collection of data and in the use or "consumption" of intelligence-related products. This frequently if not always means shifting from an emphasis on the collection of post-event evidence to: (a) the gathering, on a continuing basis, of *all* relevant data and ensuring that the data is provided for entry into appropriate databases; and (b) also drawing – from the intelligence analysts and relevant databases – all of the information needed to support ongoing operations.

Finally, adoption of the ILP process requires that senior leaders actively work with analysts and operators to ensure that the leadership is provided a clear and accurate picture of the operating environment and therefore can act to distribute resources in accordance with the reasonable conclusions and appropriate priorities developed from the data provided.

In today's homeland-security milieu, data collection and intelligence analysis are vital for the planning and prevention of, response to, and/or mitigation of terrorist attacks, man-made and natural disasters, and organized-crime incidents. Traditionally, in the United States only the armed services, the national-security intelligence community, and various specialized law-enforcement units have applied intelligence operations to their strategic-planning processes. However, because of the increasingly sophisticated operational capabilities of those who operate outside the law, it seems evident that most if not all participants in today's U.S. homeland-security efforts must use intelligence not only to improve their situational awareness but also to develop their contingency plans and determine their allocation of resources.

*J. Michael Barrett is a terrorism and homeland security expert with an extensive background in military intelligence and national security. A former Fulbright Scholar in Ankara, Turkey, Barrett is currently the Manhattan Institute's Harbinger/ICx Fellow in Homeland Security and the founder of Counterpoint Assessments, a terrorism preparedness consulting firm in Annapolis, Md.*

## Louisiana, Alabama, Washington DC, Missouri, Mississippi, and Texas

By Adam McLaughlin, State Homeland News



### Louisiana Tests Communications During Hurricane Drill

A two-day hurricane drill, carried out in late May to test Louisiana's emergency response systems in preparation for the 2006 hurricane season, determined that, although new communications systems and equipment provided by the state are working well, there are some other systems and operational areas that still need to be improved.

The exercise highlighted, among other things, the need for: (a) additional training for those involved in the management of major incidents; (b) more computers at the state emergency operations center; and (c) the use of large visual displays that allow everyone involved in the handling of major disasters to receive the same information at the same time. "Improvement also is needed in communications among various agencies and the media," said Colonel Jeffrey Smith, ANG, the state's emergency director. "There are a lot of people involved, we have to conduct more training and [improve] coordination," he stated.

Among the drill's principal successes was the performance of the new communications equipment, including three RapidCom units purchased by the state. The mobile, self-contained systems allow first responders to communicate among one another if a disaster occurs. Smith said the state's plans for the distribution of such essential commodities as food, water, and ice also checked out well during the drill. The upgraded response plan developed by the state since Hurricane Katrina also provides more staging areas, additional material resources, and more trained people to provide assistance when, where, and as needed.

On the second day of the exercise several new procedures were put into action, including the pre-positioning of National Guard units on the ground before a hurricane

makes landfall. "This year most of the Guard assets are going to be here ahead of the storm," said Terry Ebbert, director of the New Orleans Office of Homeland Security.

### Alabama Receives Initial Delivery Of FEMA Supplies

The first shipments of disaster relief supplies for the upcoming hurricane season already have arrived in Alabama. Among the supplies, provided by the Federal Emergency Management Agency (FEMA) and delivered in late May, were 57 trucks of ice (pre-positioned in Birmingham), 6,000 tarps (delivered to Selma), and hundreds of cots, blankets, and hygiene kits (stored at Maxwell-Gunter Air Force Base). These supplies, along with additional items, are important components of the state's plan to preposition emergency supplies at 31 two-year college campuses throughout the state in an innovative move to use the state's college system as a major resource for emergency shelters.

Governor Bob Riley floated the college-campus idea a few weeks earlier when acting FEMA director David Paulison was in town to participate in a hurricane drill. "We are doing everything to make sure Alabama is prepared," said Riley spokesperson Jeff Emerson. "When you have evacuees who have to stay here longer than just two or three days, we need someplace better than a gymnasium for them to sleep."

Riley's plan for a state-run system of shelters, first reported by *The New York Times*, shifts at least part of that responsibility away from the American Red Cross, which oversaw emergency shelters in the past and still will be involved in helping care for evacuees throughout the state system. "They [the campuses] are smaller, more private spaces," said Alabama College System spokesperson Amanda Vaughan. She also noted that buses from the colleges as well as security guards and nurses will help care for those who have evacuated to a campus for shelter.

## Washington DC **White House Staff Holds Hurricane Exercise**

President Bush's Cabinet tested its own ability to respond to a catastrophic hurricane during a tabletop exercise carried out late last month in a quiet office building in the nation's capital. The fictional storm, named Hurricane Boudreux, made landfall near New Orleans with sustained winds of 161 miles-per-hour.

The exercise, scheduled in part to demonstrate the administration's resolve to avoid a repeat of last year's inadequate response to Hurricane Katrina, "was a 'roll-up-your-sleeves' session in which participants dealt with difficult decisions and had frank discussions about the best way to deal with a catastrophic hurricane," said White House spokesperson Ken Lisaius.

The exercise participants dealt with evacuation and shelter plans, communications, the reporting processes and procedures for disaster managers, and coordination from Washington, Lisaius noted. "We are working," he said, "to implement the lessons learned from Katrina and this exercise helped us evaluate the needs as this hurricane season approaches."

The drill, which was carried out in the Eisenhower Executive Office Building, was the third in a series of tabletop exercises in the last six months intended to simulate the Cabinet's role, responsibilities, and lines of authority in responding to a catastrophic national incident. The first two drills dealt with the possibility of a pandemic flu and the management of a smallpox outbreak.

## Missouri **Expands Explosive-Detection Capabilities at Kansas City International Airport**

The Transportation Security Administration (TSA) has announced the deployment of five Reveal Explosive Detection Systems for screening checked baggage at the Kansas City International Airport. "This is an example of our continuing effort to develop and deploy the latest technology," said TSA's Richard Curasi, federal security director at the airport. "[It] is the latest tool we can use to secure our passengers," he said.

The Reveal CT-80 machines are smaller and less than half the price of other explosive-detection machines currently in use at commercial airports throughout the United States. Because of its smaller size and weight, the Reveal CT-80 requires fewer terminal modifications and can easily be installed behind airport ticket counters, with minimal construction or additional infrastructure required. The low unit cost and reduced infrastructure requirements make the product a cost-effective alternative to many of the other explosive-detection systems now on the market and/or in use at a number of other airports.

*Because of its  
smaller size and weight,  
the Reveal CT-80  
requires fewer terminal  
modifications and  
can easily be installed  
behind airport  
ticket counters*

Last year, TSA installed eight Reveal machines for operational testing and evaluation at three airports. Following the success of the pilot program, the agency purchased 72 Reveal machines at a cost of \$24.8 million with the goal of deploying the equipment to small and medium-sized airports during the first half of 2006.

## Mississippi **Storm Plans Incorporate Public-Private Partnership**

During a hurricane-planning session on June 12, mayors and emergency responders from towns in southern Mississippi met with Wal-Mart representatives to develop an organized response in preparation for the 2006 hurricane season.

Wal-Mart officials asked each locality represented to provide a list of contacts and emergency supplies that would be needed after a storm. Brian Thomas, who manages the Wal-Marts in South Mississippi, provided the

company's own contact numbers to the local officials. Hurricane Katrina demonstrated the ability of Wal-Mart, the world's largest retailer, to move large quantities of essential supplies and equipment into a stricken area on very short notice. "We have the finest logistics network in the world," said Thomas. The company also has the largest privately owned trucking fleet in the United States.

Wal-Mart officials said the company also is working with the Salvation Army and the American Red Cross to ensure that emergency needs are met at evacuee shelters and other sites. Wal-Mart already has promised to make its parking lots available for use as relief distribution sites. Store representatives also told the workers and supervisors who will be on the front lines of the next hurricane emergency that the company wants to help in any and every way possible in the hours immediately after a storm. Company stores that do not open immediately, officials said, will be used as pick-up sites for water, ice, and other essential supplies such as personal hygiene items and non-perishable food.

Ocean Springs Mayor Connie Moran wanted to know if Wal-Mart would help out at other emergency sites. "We [Wal-Mart] are set up at Ocean Springs Middle School, for example. That was our ice-and-water distribution point, and we also used it as a secondary emergency operations center. ... Can we count on you," she asked, "to deliver water and ice immediately, even before the FEMA, MEMA, [and] Red Cross people come in? If we have the resources, then I have the authority to tell you we will get it there as fast as we can."

"But who knows how fast that is," Thomas answered. He said the company is coordinating with its vendors across the country to stockpile water and ice so that those essential commodities can be trucked in, wherever they are needed, as soon as possible after a major storm hits.

## Texas **Plans to Install Web Cameras Along Border With Mexico**

Texas Governor Rick Perry has announced a \$5 million plan to install hundreds of night-vision cameras on privately owned tracts of land along the Texas border with Mexico, and to put live-video footage of intrusions on the



internet. The intent of the project is to allow anyone with a computer who spots illegal immigrants trying to slip across the border to call in on a toll-free hotline.

Perry said that the state plans to pay for the program with grant money that Texas already has received, and added that he wants the first cameras in place by the middle of July. "I look at this as not different from the neighborhood watches we have had in our communities for years and years," Perry said.

The camera plan marks a political about-face for Perry, a Republican seeking re-election, who previously took the position that security along the state's 1,200-mile border with Mexico is strictly a federal responsibility. Cuts in federal homeland-security funding, a rise in reports of border violence, and the crossing of Mexican soldiers into Texas about two years ago have demonstrated, though, Perry said, that "Texas cannot wait for Washington, D.C., to act."

Under the plan announced in early June, cameras and other surveillance equipment would be supplied to willing landowners and installed along some of the most remote stretches of the Texas/Mexico border. The live video would be made available to law-enforcement agencies, and to any agency or private citizen with an internet connection. Viewers would be able to call in, day or night, to report anything that looks like trespassing or drug smuggling, or seems suspicious in various other ways.

Some critics are contesting the governor's plan, describing it as "dangerous" and/or "a waste of money." "This is just one of those half-baked ideas that people dream up to save money but have no practical applications," said James Harrington, director of the Texas Civil Rights Project. "We would be far better off to invest that money in Mexican small towns along the border so people would not have to emigrate."

*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.*

## Terrorism: The Cyberspace Battleground

By Thomas Kellermann, Cyber Security

The information age and the increasing capabilities of computer networks have led to technological breakthroughs never before possible – including some that have been exploited not only by everyday criminals, but also by terrorists. The dimensions of what is now a huge and growing problem – for homeland-security and law-enforcement agencies both – were spelled out, in fact, in a 2006 Federal Bureau of Investigation cybercrime study which noted that 90 percent of U.S. businesses were affected by cybercrime last year in one way or another, and the overall economic cost to the United States is now close to \$70 billion annually.

The inherently transnational nature of the Internet makes it an ideal vehicle for those, including criminals, who seek to maximize profits with an acceptable degree of risk. The conventional view of the lonely teenager or computer programmer as the source of malicious code such as the MiMail virus is often incorrect. In today's climate, the hackers associated with major cybercrimes are often working with cyber syndicates, including many in Eastern Europe. Some of the most successful of these crews have been traced to Russia, Romania, Ukraine, Estonia, Latvia, and Lithuania.

The key personnel in these syndicates are professional hackers, available for hire. Eastern Europe boasts a plethora of people who possess advanced computer skills but do not have legal opportunities to use those skills to make a living. The alternative for them has been cybercrime. Many if not all of the early virus writers used to write code for the art of it, and/or to impress their peers. But they eventually realized they could make a lucrative living from their highly specialized capabilities.

### Anonymity and Invisibility

There are several other factors that seem to have made Eastern Europe a major center of hacker activity. Governments are sometimes unstable, and there is a high unemployment rate – but the workforce is highly educated, there is widespread criminal activity of other

types, and a thriving underground economy. Unlike a Mafia group that keeps criminality within an extended family, Eastern European groups tend to act more like trusted merchants on a silk road. Moreover, in the post-Cold War era, individual citizens usually are not tracked by any central authority.

In addition, the ability to maintain anonymity online is taken for granted, and permits hackers to work closely with other hackers, possessing similar skills, whom they have never met. The hackers and/or hacker teams can launch attacks from computers thousands of miles away from their victims, and can use a long chain of several compromised computers to hide their tracks.

Today's Internet criminals have extended the turf of what law-enforcement agencies have traditionally called the Mafia. They have adapted their goals and methods of operation to new types of crime, shifting from the numbers and narcotics rackets of the mid-20th century to Internet identity theft and denial-of-service (DOS) attacks.

### Smarter and Better Organized

The current and future generations of would-be criminals are and will be computer-literate, and can be expected to use their high-tech computer skills both extensively and successfully. All evidence suggests that there are not only more and more cyber criminals now than ever before, but also that the worst of these criminals, the cyber terrorists, are becoming much better organized and more coldly methodical in their modes of operation.

This is a major change, with ominous implications for all nations of the Free World. When the first federal cybercrime laws were enacted in the early 1980s, U.S. law-enforcement and intelligence agencies found that the majority of their cases involved hackers who were breaking into computers mostly to claim "bragging rights" – i.e., to impress other hackers. Many developing countries are quick to embrace technologies, such as wireless, because of the potential benefits

they offer. These technologies frequently are adopted without proper consideration to, or understanding of, the inherent risks. Or countries adopt inherently risky technologies, relying on single silver-bullet solutions such as firewalls or encryption to mitigate all risks rather than adopting a multi-layered approach that secures each component of the technologies in play.

Moreover, because of limited public access to information technology, a number of developing countries provide online services to deliver personal information and services through public kiosks, Internet cafes, or other public spaces where several persons use the same computer. Consumers use these computers without realizing that they may be bargaining away not only their privacy, but also the confidentiality and integrity of their personal information, in return for convenient access, speed, and reduced cost.

### ***Built-In Institutional Handicaps***

A major problem is the lack of public awareness of the dangers inherent in the digital environment. Many developing countries either do not have, or do not properly use, the educational materials required to properly train citizens about the complexities of inherent risks and mitigation techniques. As a result, users do not take the steps needed to mitigate threats in the online environment so that commerce can continue with minimal risk.

Simultaneously, a senior-level lack of awareness is proving to be a key limitation for e-security managers and other professionals. Without proper education, system administrators and law-enforcement personnel in emerging countries can face a critical handicap in their ongoing security efforts. This serves to weaken their technological infrastructures, making them vulnerable to cyber attacks.

Many developing countries lack the institutional structure to implement, monitor, and enforce proper e-security measures. Laws, specifically including those involving cyber crime and/or e-commerce, must be revised to create better incentives for proper e-security. Furthermore, even if the laws and regulations are adequate, a deficiency in enforcement capabilities can greatly hinder their effectiveness.

Today it can be taken for granted that what affects networks in Romania eventually will

affect networks in other countries – including the United States. As is the case with organized crime, terrorists are becoming more sophisticated in their ability, and willingness, to use hackers in their war against the West. Better educated than their forebears, but motivated by the same hatred of Western culture, the new generation of terrorists can move quickly and virtually through cyberspace to strike at the very heart of the Western economic infrastructure.

Another major concern for homeland-security professionals, and for political decision makers, is that criminal and terrorist operations may converge as the terrorist motivation shifts from destroying the infidel economy to controlling it. The capitalist market thus would become the funding mechanism to support traditional terrorist tactics. As a result, organized crime, terrorists, and the state sponsors of terrorism may well be able to operate in the same environment, ultimately negotiating for control of and access to financial information and the funding it provides for their respective activities.

***Cyber terrorists  
are becoming better  
organized & more coldly  
methodical in their  
modes of operation***

### ***A Harbinger Of Future Nightmares***

An ominous harbinger of greater dangers ahead is that the Internet already is being used to gather information on potential targets. The website operated by what U.S. intelligence agencies call the “Muslim Hackers Club” reportedly featured links to U.S. sites that disclose sensitive information such as code names and the radio frequencies used by the U.S. Secret Service. The same website offered tutorials in hacking.

The Internet is a true force mobilizer and force multiplier for non-state actors. Ronald Dick, former director of the FBI’s National Infrastructure Protection Center, said that he considered the theft of or manipulation of data by terrorist groups to be his worst

nightmare, and was particularly concerned by the possibility that cyber attacks might be merged with physical attacks on infrastructure targets such as the power grid. As a result of the increasing U.S. dependency on cyberspace, consumers can no longer detach themselves from the electronic crimes that are committed overseas. Law-enforcement agencies must cooperate across national borders in order to slow the tide of cyber crime. The Internet has become the vehicle of choice to coordinate crimes and launch attacks against Western societies.

For international law-enforcement agencies to counter what might otherwise be a cybercrime epidemic, several important steps must be taken, among them the following. First, all nations must ratify the Council of Europe Convention on Cybercrime. In November 2001 the Council of Europe approved a treaty to foster cooperation between sovereign states and the private sector in combating cybercrime and to protect legitimate interests in the use and development of information technologies. One of the principal tenets of the treaty was that to effectively combat cybercrime would require increased, rapid, and well-functioning international cooperation in criminal matters. The United States has yet to ratify the treaty.

Second, international institutions must work together in creating a “culture of security” by allocating grants for cyber forensics training for the law-enforcement agencies of developing countries. Lastly, the Internet Service providers of the world should maintain their log files for a minimum of one year so that trails remain for global investigations.

If the recently revealed U.S. Veterans Administration data breach symbolizes anything, it is that personal information has become an increasingly lucrative commodity. Cybercrime is in that context not really new, but merely a much more effective vehicle that can be used by organized criminals to carry out their illegal activities. A respect for their level of sophistication and tactics needs to be earned if the world is to slow this virtual scourge.

---

*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).*



# 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

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](mailto:subscriber@domprep.com)

**FREE** to Qualified Professionals



**DomPrep Journal**  
Management Solutions

410.518.6900  
[www.DomPrep.com](http://www.DomPrep.com)

The IMR Group, Inc. publishing DomesticPreparedness.com (DomPrep) since 1998 to integrate the diverse first responder communities of state, local, national, 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 JTFs - "Jointness" at Its Most Effective!

By Christopher Doane, Joseph DiRenzo III, and Jeffrey Robertson



The term "joint" is usually used in discussions about the nation's armed forces, including the U.S. Coast Guard, and how they are now operating more closely with one another than ever before.

Today, each service brings its own unique capabilities, experience, and equipment to the table, presenting a formidable front to carry out an increasing number of multi-service tasks.

In the post-9/11 security regime it is not surprising that the idea of jointness has extended to fighting terrorism by using the combined capabilities of federal, state, and local law-enforcement agencies. The federal government has found that success against terrorism is best achieved through close cooperation among the various stakeholders involved. To be truly effective, though, this cooperation must go beyond discussions about the need to exchange information, and into the fields of planning and operations.

One of the most successful examples of implementing this principle is the FBI's Joint Terrorism Task Force (JTTF), which combines federal, state, and local law-enforcement agents and analysts into a single unit – working, almost always, under the leadership and guidance of a local FBI field office. The idea of creating an FBI-led task force, first used in New York City in 1979 to deal with bank robberies, proved to be such a valuable investigative tool that it started to be used in counterterrorism operations the following year, 1980.

## *A Constellation Of Experienced Professionals*

Today, JTTF operations are carried out by just over 100 geographically based task forces, which for operational and chain-of-command purposes report to and through the 56 local FBI field offices scattered throughout the nation; each field office has at least one JTTF under its jurisdiction.

To provide program management and support of the field-office JTTFs, a National Joint Terrorism Task Force (NJTTF) has been established within the Counterterrorism Division (CTD) at FBI headquarters in Washington. That office – which is staffed with FBI agents and analysts and approximately forty liaison officers and agents from the intelligence, law-enforcement (state, local, and federal), and public-safety communities – has been assigned the unique responsibility of multi-agency information collaboration and sharing.

The NJTTF also sponsors a fellowship program that brings state and local law-enforcement agents to FBI headquarters to learn the counterterrorism program at the national level and, in return, provide local perspectives to national initiatives. Here it should be noted that, although the NJTTF provides programmatic oversight and resource support, the local FBI field offices retain operational oversight of local JTTF activities.



# Maritime Security Expo 2006

*5<sup>th</sup> Annual Expo & Conference*

September 19-20, 2006

Jacob Javits Convention Center, New York City

**The Largest Maritime Security  
Event in the World**

**For more information on exhibiting or sponsorship opportunities, please  
contact Barbara Lecker, Derek Lotfi or Anna Grapek at 301-493-5500.**

**[www.maritimesecurityexpo.com](http://www.maritimesecurityexpo.com)**

Organized By:



**E. J. KRAUSE &  
ASSOCIATES, INC.**

**Corporate Partner:**

Lockheed Martin

**Corporate Sponsors:**

SeaAway

IBM

Booz Allen Hamilton



## **Investments, ROI, And More Convictions**

The JTTFs obviously represent a significant investment of both personnel and equipment. The nation's return on that investment also is significant, though, and comes in the form of numerous improvements in interagency coordination and cooperation, a greater sharing of intelligence, and – most important of all – a major increase in arrests and convictions of those apprehended through counterterrorism investigations.

The mission of the “typical” JTTF is to organize, and coordinate the efforts of, federal, state, and local law-enforcement agencies that have joined forces for the purpose of preventing, deterring, defeating, and responding to any terrorist attack within the United States. Close coordination with first responders and appropriate principals in business, industry, and the local community in planning, training, and exercising is critical, of course, to implementation of a successful federal counterterrorism program.

The FBI defines terrorism, on its official website, as “the unlawful use of force or violence, by an individual or individuals, against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.” Beyond these broad areas of emphasis, the JTTFs also focus on special events and activities, symbolic targets, and/or critical infrastructure that could serve as particularly attractive targets for terrorists.

For terrorists, attacks against major special events not only could cause a significant loss of life, but also could create psychological trauma and would attract a high level of media exposure. In recognition of these potentially disastrous consequences, the JTTFs already have been called out in force to help in coordinating the FBI's security preparations for the Olympic Games, several Super Bowls, the 2004 presidential nominating conventions, and a number of national and international conferences.

Although many of their successes are highly classified, it seems clear that the JTTFs have become a particularly useful counterterrorism

tool, and have played a critical role in many significant terrorism investigations. Among the better known JTTF contributions are the conviction of Ramzi Yousef and Eyad Mahmoud Ismail for conspiracy in the February 1993 bombing of the World Trade Center, and the arrest and prosecution of the shoe bomber, Richard Reid.

*Each service  
brings its own unique  
capabilities, experience,  
and equipment  
to the table*

## **A Few Problems, And Some Possible Solutions**

Obviously, there is always room for improvement and greater synergy even in a well-functioning law-enforcement organization. Following is the background on certain problem areas and/or possible changes in the NJTTF/JTTF organizational structure and/or operational philosophy that have been recommended for consideration by national decision makers:

1. The success of the local JTTF is directly related to the level of participation and “buy-in” by local law-enforcement agencies. But it is often difficult for smaller agencies to provide a full time member to the local JTTF. This problem is exacerbated because of military reserve recalls and overall difficulties in recruiting (caused, at least in part, by low entry-level salaries). “Losing” a member to a local JTTF is frequently perceived, therefore, as a problem rather than an opportunity. One possible solution is to provide federal funding support to smaller law-enforcement agencies.
2. Top-level organizational support also is needed to improve the two-way information exchange – which too often is viewed as state and local jurisdictions providing information to the FBI but receiving little or no information from the FBI. (Other federal agencies have voiced the same complaint from time to time.) One solution here would be to develop a system similar

to the one used by the Coast Guard, which under federal law permits its Captains of the Port to share sensitive security information (SSI) not only with other agencies but also with the private sector. Under this carefully controlled information-exchange system, representatives of other law-enforcement agencies, and from the private sector, who are considered as having “a need to know” are designated “covered persons” (but only after screening and familiarizing themselves with the protection requirements for SSI materials, as also set forth in various federal regulations). The ability to share essential information not only builds trust between and among stakeholders but also contributes significantly to the synergistic capabilities of the JTTFs involved in specific operations.

3. Despite the broad spectrum of agencies involved, the JTTFs are not always as flexible as they perhaps should be, and some are considered to be actually quite rigid in their method of operations. That inflexibility could be a major disadvantage in operations against the dynamic and asymmetric terrorist threat. Greater vision is required by leadership at all levels to allow the organizational structure of the JTTFs to have more latitude in responding to the changing nature of the threat.
4. Investigative efforts must not over-emphasize threats originating from overseas vice attacks initiated from within the United States itself. Much of the NJTTF's focus to date has been on preventing evildoers from entering the country. However, numerous reports have suggested that a number of terrorist cells already exist within the United States, and the threats represented by those cells are at least as dangerous as the threats posed by terrorist infiltrators coming in from overseas.

---

*Christopher Doane (pictured on previous page), Joseph DiRenzo III, and Jeffrey Robertson are retired Coast Guard officers. Doane and DiRenzo are now Coast Guard civilian employees, and Visiting Fellows at the Joint Forces Staff College. Robertson's last assignment was as Coast Guard liaison to the FBI; a former member of the NJTTF, he is now a maritime-security and antiterrorism consultant with Whitney, Bradley & Brown Inc. in Vienna, Va.*

## Toronto and the U.S. Canadian Border: What Should and Should Not Happen Next

By Joseph DiRenzo III and Christopher Doane



The arrest of 17 suspected terrorists in Canada last weekend has added additional fuel to the call for increased security along the U.S. – Canadian border.

But that would be only part of the answer – and not the most important part, according to at least some senior-level officials and private-sector experts. Instead, these sources say, the two nations should be working primarily to achieve greater cooperation and more transparency between U.S. and Canadian security agencies. The joint goal should be to ensure the security of the U.S. and Canadian external (i.e., maritime and air) borders while leaving their shared internal border relatively open.

The 5,000-mile border between the United States and Canada – the longest non-militarized border in the world – logs over

200 million crossings per year. The border's openness supports and facilitates a significant bilateral flow of goods and services valued at more than \$1.2 billion per day and responsible for over five million jobs in the United States alone. To cross the border, U.S. and Canadian citizens need only a valid driver's license and a copy of their birth certificate.

Recently, in large part because of the debate over illegal immigration across the U.S.–Mexico border, there have been calls for tightening the U.S.–Canadian northern border as well. However, as senior officials realize, the only known attempt by a terrorist to cross into the United States from Canada in recent years was the Millennium Bomber, Ahmed Rissan, who was captured in Port Angeles (Wash.), with a trunk full of explosives in December 1999.

### *The Real Factors Involved*

There is another significant political, economic, and national-security factor to consider. The key issue in the U.S.–Mexican border controversy is illegal immigration. The government of Mexico seems either unable or perhaps unwilling to control the flow of migrants through and from its own territory into the United States – which therefore has no choice but to deploy enough manpower (and high-tech equipment) along the border to at least reduce the tremendous flow of illegals to help ensure the economic integrity and homeland security along its southern border.

U.S. security officials are of course also aware that terrorists might try to mix into the flow of illegal migrants to infiltrate the U.S. homeland, but the primary concern – at the present, at least – is the impact of so

## ARE YOU PREPARED FOR A CHEMICAL ATTACK?

Do you have the proper equipment, training, and knowledge?

### Responding To A Chemical Event WebConference

View "As-If Live" presentations by knowledgeable speakers as they discuss in-depth training, technology procedures, and other pertinent information that is essential to all preparedness professionals.

**\*FREE Registration**



Visit [www.DomesticPreparedness.com](http://www.DomesticPreparedness.com) for more details

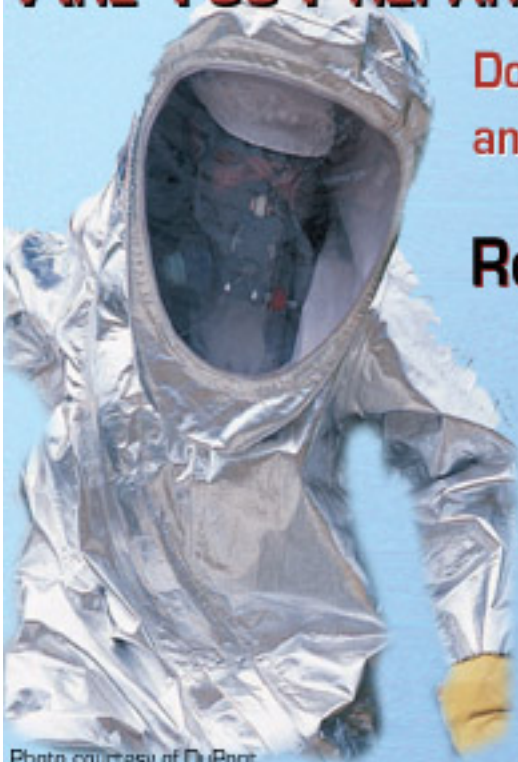


Photo courtesy of DuPont



many millions of migrants on the nation's economic security.

Canada, on the other hand, has a stable government very much in control of its own territory and policies. It is a nation, moreover, that has long demonstrated a spirit of strong cooperation and coordination with the United States. Beginning with the Permanent Joint Board on Defense formed in 1940 and NORAD (the North American Aerospace Command) in 1958, U.S. defense arrangements with Canada are closer and more extensive than with any other country in the world.

The cooperation between the respective law-enforcement agencies of the two nations has also been excellent – and has improved significantly since the 9/11 attacks (following which Canada strengthened its own anti-terrorism laws). Certainly, the arrest of the 17 terrorists outside of Toronto is clear evidence of the effectiveness of Canadian law-enforcement agencies in the fight against international terrorism.

### ***Foreign Terrorists, But Local Materials***

Any valid discussion of security changes along the northern border requires a clear understanding of the real threat. A merely cursory review of the 1993 bombing of the World Trade Center in New York, the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, and now the arrest of the 17 terrorists in Canada shows that, *in each case*, the terrorists obtained (or were planning to obtain) locally available materials to make their bombs.

Locally obtained materials also were used by Japanese terrorists for the 1995 Sarin Gas attack on the subway in Tokyo, and the U.S. passenger aircraft planes used in the 9/11 attacks also were “obtained” locally. This strongly suggests that the preferred modus operandi for would-be terrorists is to rely on locally available materials to build their weapons of mass destruction. The exception, perhaps, would be the use of more complex weapons (nuclear, radioactive, and biological) – but these have yet to be employed by terrorists and must be considered low probability for at least the present. Which is not to say that terrorists would not be willing to

use weapons of mass destruction against the United States and its allies – if those weapons were available.

***The two nations  
should build on their  
already strong  
working relationship  
by creating a new  
joint security program***

Because of the apparent need for terrorists to obtain their weapons locally, the predominant threat at the northern border is not the transport of weapons or weapon-making materials, but the movements of terrorists themselves. That would not be true if the effectiveness of Canadian security forces in detecting and stopping internal and external threats were considerably less than the U.S. capabilities. Here it must be recognized, though, that the position of at least some of those who argue for tightening U.S. security along the northern border is that Canada's immigration policies and external border-security measures are relatively weak.

### ***Building on Strength***

Even if it *were* true that Canadian border security is weaker than that of the United States, though, tightening security along the northern border, thereby significantly impeding the flow of trade between the two nations, is not necessarily the best answer. Instead – again, in the opinion of some senior leaders – is that the two nations should build on their already strong working relationship by creating a new joint security program that tightens the security of the external U.S.-Canadian land borders and improves their respective ability to detect and stop cells already operating within the United States and Canada.

The political and military leaders of both nations also should communicate their concerns with the other's external security measures and, if necessary, seek satisfactory solutions to any problems that exist. If the primary U.S. concern is terrorists entering

the United States through Canada, then that should be the principal area of focus. But it is obviously less urgent to provide additional internal border security if the external borders of both countries are already reasonably secure, the U.S. and Canadian internal security systems are sound, and there is enough transparency and cooperation between and among agencies to instill mutual trust and confidence.

One excellent example of how mutual security between the United States can and does work is the Joint Initial Verification Team, or JIVT – a partnering of U.S. Coast Guard and Transport Canada inspectors to conduct joint security inspections of vessels bound for the Saint Lawrence Seaway and U.S. or Canadian ports in the Great Lakes. These joint inspections eliminate the redundancy that would slow commerce while also providing both nations with the confidence needed to allow the vessels to enter their ports. Canadian officials are also working closely with the U.S. Customs and Border Patrol in the Customs-Trade Partnership Against Terrorism (C-TPAT) program and the Container Security Initiative (CSI).

These joint security ventures serve as impressive models of how the United States and Canada should move forward. The exchange of additional liaison officers between border security agencies to monitor security operations, providing even greater transparency, would inspire even greater mutual confidence. Collectively, these and similar actions seem to promise a far more cost-effective solution than spending billions of dollars to flood the U.S. northern border with Canada agents and sophisticated electronic systems that might and probably would help tighten security to at least some extent, but also would have a negative impact on trade and weaken the 200-year tradition of openness between the two countries.

*Joseph DiRenzo III (pictured on previous page) and Christopher Doane are retired U.S. Coast Guard officers now employed as Coast Guard civilians and are Visiting Fellows at the Joint Forces Staff College. The opinions they express here are their own and not necessarily those of the publisher or of the U.S. and/or Canadian governments.*

## Anatomy of an Exposition

# The IED Problem: Solutions On Display, and On the Way

By Robert Besal, Viewpoint

Enhancing the force protection and survivability of U.S. soldiers and Marines was the primary focus of the IED 2006 Symposium & Expo earlier this month at the Crown Center in Fayetteville, N.C. More than 600 attendees and 48 exhibitors participated in the mid-June event, produced by Lodestar Group, a defense marketing firm based in Raleigh, N.C. "Our goal was to bring together the innovators who develop and produce counter-IED technologies and equipment with the front-line operators," said Catherine Vilga, president of Lodestar Group. "Based on our attendance statistics as well as exhibitor feedback, we certainly succeeded," she said.

Improvised explosive devices (IEDs) have caused over 890 U.S. deaths and more than 16,000 total casualties since July 2003, and are considered the greatest current threat to U.S. troops deployed to Iraq and Afghanistan. But Expo attendee Detective Leroy E. Morgan Jr. of North Carolina's Hoke County Sheriff's Department said that IEDs pose a serious threat to stateside law-enforcement officers as well. "Unfortunately, even little towns like ours are going to need some of this equipment [on display at the Crown Center Expo] in the next five to ten years," he commented. "We have no reason to believe" that the IEDs "won't find [their] way over here."

Lieutenant Colonel Patrick Kelleher, USMC, and Lieutenant Colonel Randy Powell of the North Carolina Army National Guard, combat-experienced battalion commanders who recently returned from Iraq opened the symposium by providing their joint warfighters' perspective. They also fielded questions from other symposium attendees, many of whom noted that it was the first time they had actually had a conversation with a company commander about front-line requirements.

Kelleher elaborated on the symposium theme – "Breaking the Chain" – by discussing the motivations and operating tactics of the insurgents. He identified the principal steps in the IED attack process as construction, placement, and deployment, and encouraged his audience to concentrate their efforts in

the corresponding countermeasure areas: using improved intelligence to prevent the building and assembly of IEDs; developing better sensors to detect emplaced bombs; and enhancing group and individual protection through the production and distribution of better armor and the use of various other adaptive technologies.

### The Prerequisites for Mission Success

Another speaker, Marine Colonel Brian Green of the Department of Defense's recently-established Joint IED Defeat Organization (JIEDDO), also provided an IED update briefing that included relevant JIEDDO organizational information as well as a "past, present, future" perspective of the IED threat. He also participated in a later symposium session to discuss the technological challenges that JIEDDO believes must be overcome to ensure mission success in an IED environment.

Many exhibitors commented favorably on the marketing opportunities presented by the sizable active-duty military audience participating in the seminars and visiting the Expo exhibitor booths. AMTI demonstrated the company's remote-controlled robot, which is equipped with a high-resolution camera that can be used to inspect and disable potential explosive devices. Another remotely operated vehicle, developed by NIITEK, featured a modified commercial chassis carrying a mine-search system that uses a front-mounted ground penetrating radar that can "see" several feet into the earth to detect buried explosives. Among the many other products on display were the Force Protection Industry's armored transport vehicle, the MUV-R, and a never-before-exhibited bomb-resistant guard post provided by Law Enforcement Associates.

The second day of the symposium featured panel presentations bringing together speakers from several of the nation's most highly respected academic and commercial research institutions, including the Johns Hopkins University's Applied Physics Laboratory, the Georgia Tech Research Institute, SRI (formerly Stanford Research Institute), and the MITRE Corporation. A number of industry representatives, from companies both



New multi-use AMTI Robot finds and kills IEDs.

small and large, discussed various emerging technology concepts and recommended ways to negotiate the requirements process more quickly in order to move innovative products from initial concept to front-line users as rapidly as possible.

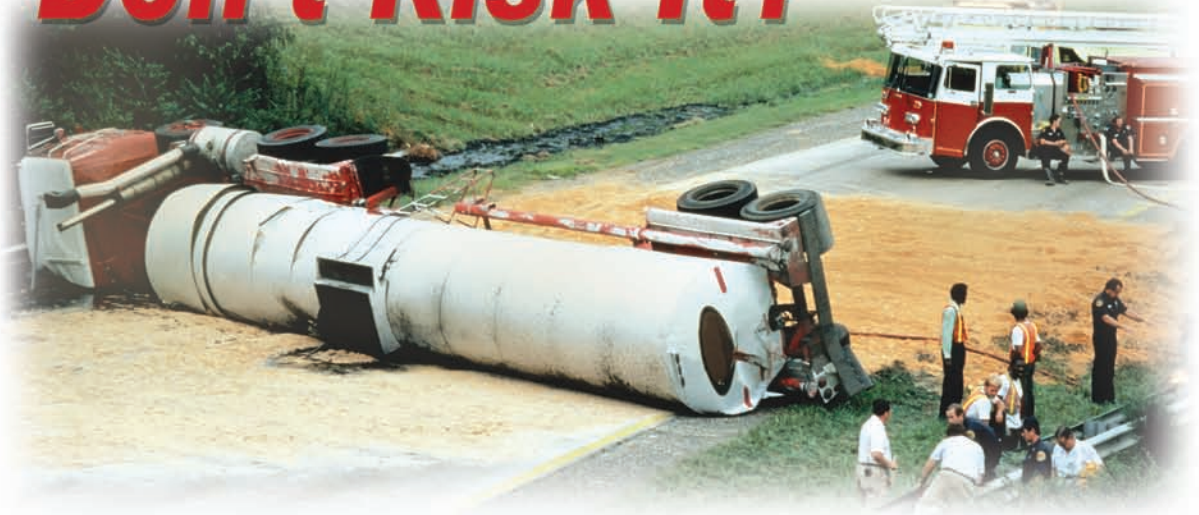
One of the most-discussed presentations was provided by Marvin Leibstone, an internationally respected writer and commentator now serving as editor of *Global Security & Trends Journal*. After pointing out that the U.S. and allied counter-IED programs have been underfunded for years, Leibstone also noted that the insurgents in Iraq have, in contrast, steadily increased and improved their own IED capabilities and techniques. One important result, he said, has been the growth of a burgeoning anti-war movement in the United States itself.

The Expo's proximity to nearby Fort Bragg and Camp Lejeune provided exhibitors and symposium attendees with numerous opportunities to interact directly with the soldiers and Marines who are the end-users of the products and services that were on display. "We seldom hear from the actual boots-on-the-ground about the usefulness or supportability issues with our products," said exhibitor Henry Turtle of Scanna MSC. "By the time we get feedback from the field, it's months later, and the word has often filtered through many layers. This conference has been invaluable."

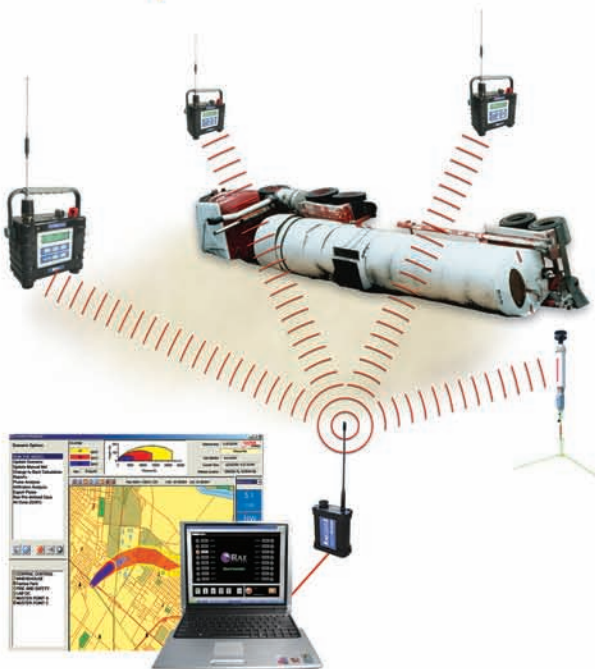
*Rear Admiral Robert E. Besal, USN (Ret.), a former naval aviator, served in a variety of sea and shore assignments around the world during his 30-year career, including duty as commanding officer of the aircraft carrier USS America. He is now Executive VP, overseeing all program development, for Lodestar Group LLC and defensetradeshows.com.*



# ***Don't Risk It!***



***There's a deadly chemical release.  
Why trust your safety – and the public's safety –  
to a product without a track record?***



## **AreaRAE** **Wireless HazMat Detection**

- Remotely measures gas, vapor and radiation threats from up to two miles away
- See the entire threat from Incident Command
- With over 500 systems deployed, the AreaRAE is the standard for rapid deployment systems

### **Used by:**

- Fire Departments
- Law Enforcement
- Industrial First Response Teams
- State and Federal Agencies

[www.raesystems.com/info](http://www.raesystems.com/info)

**Protection through Detection**

