domestic preparedness .com

DomPrep Journal

US $75 Annual

Volume II, Issue 2, January 25, 2006

Big Push for Maritime Security

USCG Expands Far East Operations

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 Coordinator
sstovall@domprep.com

Paige Dunn
Customer Service Coordinator
pdunn@domprep.com

DomPrep Journal is electronically delivered 26 times per year by the IMR Group, Inc., 517 Benfield Road, Suite 303, Severna Park, MD 21146, USA; 410-518-6900; fax 410-518-6020 and available at DomPrep.com

Articles are written by professional practitioners in homeland security, preparedness, and other 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 Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher.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.

IMR Group

Editor's Notes

By James D. Hessman, Editor In Chief

The world will never be safe from international terrorism until the citizens of all free nations throughout the world will work as hard to preserve civilization as terrorists and other evildoers are working to destroy it.

That is the implicit message in Managing Editor John Morton's insightful essay in this issue of *DPJ* discussing the sometimes unwitting but always harmful anti-democracy role played by such "failed states" as Somalia and Sudan that provide safe harbor and other support to Al Qaeda and other terrorist groups. The activities of those groups, and of the several economically and politically bankrupt nations that give them so much aid and comfort, should be of growing concern not only to U.S. diplomats and the nation's armed forces, but to state and local law-enforcement agencies as well and to all first responders everywhere.

The fact is, as Morton points out in his essay (which substitutes in this issue for his customary interview), that the malicious and destructive plots and schemes created by Al Qaeda leaders in the caves of northern Pakistan are later refined and developed in minute detail in safe houses in London or Munich – and eventually are carried out in the cities of America and Europe by younger and even more fanatical terrorists living in the apartment "upstairs from the Laundromat." Again, homeland defense begins overseas, and sometimes halfway around the world.

It often has been said, with rueful humor, that no good deed goes unpunished. The same is true of technology. The rapid advances in communications technology, in transportation and logistics capabilities, and in medicine and so many other fields of science during the last century and the early years of the 21st have benefited the citizens of all nations. But the tools of human progress are always dual-purpose, and can be used not only to help man in his long upward struggle toward the light but also to hinder him.

The increased use – i.e., the misuse – of the Internet and other IT systems by terrorists and hackers to disrupt and disorient both public agencies and private businesses is but the latest example of how otherwise benevolent technology can be used to create economic panic as well as political chaos. Thomas Kellerman, one of several new authors in this issue of *DPJ*, addresses that important topic with both knowledge and wisdom.

Not all is gloom and doom, though. Joseph Cahill points out that today's generation of emergency medical services personnel are not only better and more professionally trained than their predecessors, they also (finally) are better equipped as well – starting with the new "hospital on wheels" types of ambulances they are being provided. And two other new authors, Christopher Doane and Joseph DiRenzo III, team up in an encouraging report on how U.S. Coast Guard personnel and their Customs and Border Patrol counterparts are working throughout the Far East to sanitize U.S.-bound ships and cargo containers at their point of origin, rather than in the seaports of America.

A Request to *DPJ* Readers: A new "Readers' Notes & Comments" is scheduled to debut in the next issue (8 February) of *DomPrep Journal*. Contributions are hereby solicited. The letters and emails submitted should be addressed to (feedback@domprep.com), run no longer than about 150 words, comment on recently published articles and/or suggest other topics that might be of interest to the magazine's readers.

Cover: The tug and barge Takamatsu Maru pushes the U.S. Coast Guard cutter Jarvis into her berth at the Japan Coast Guard's Maritime Disaster Complex in Yokohama at the start of the Jarvis's visit to Japan last year as part of a bilateral agreement. USCG photo by Amy Thomas.

Analysis and Commentary

Terrorist Networks, LE, and The Relevance of Failed States

By John Morton, Commentary

At state police headquarters, the criminal intelligence section received a tip from a Laundromat manager – Hispanic – that a group of young men (West Africans, said to be from Nigeria) had moved into the upstairs apartment and were acting suspiciously. Sometime later, a patrol officer determined that the men were West Africans from Ghana. It was not known whether they were students or perhaps employed either full– or part-time. The still unanswered question was whether, solely on the basis of the information provided, the young men should be considered a security threat.

In a December 2005 DomPrep interview, former Director of Central Intelligence (DCI) R. James Woolsey said the front line of intelligence-gathering in the war against terrorism is at the local level. He also provided a number of examples similar to the one above. Local law enforcement (LE) knows its territory best, he commented, and through good police work is better able to recognize anomalies that might indicate terrorist activity. Somewhat ominously, he also emphasized that local authorities should not assume that the federal-level intelligence community is going to be of much help in providing actionable intelligence indications and warnings (I&W) to local LE agencies. Just the opposite, in fact. On balance, he suggested, the flow of I&W information could easily be upward – from local to federal.

Local LE agencies have always had to be aware of the larger context in which they operate – and today that context is inescapably global. So the question remained: Are the Ghanaians likely to be terrorists? There is a related question of a more practical nature: Given the fact that police resources are almost always scarce, how much manpower and/or other assets should the department allocate to determine the answer to the first question? Here, a relatively quick answer could be developed by knowing a little more about Ghana itself – e.g., whether it is, in fact, what is called a "failed state."

Breeding Grounds for Catastrophe, Destabilization

The term *failed* state gained considerable traction in Washington after 9/11 when the White House's 2002 U.S. National Security Strategy document concluded that "America is now threatened less by conquering states than … by failing ones." In a failed state, a government has lost control of its territory and lacks the authority to make collective decisions and/or the ability to deliver public services. As for the populations of failed states, they may refuse to pay taxes; they may participate fully in the black-market economy; or they may engage in large-scale civil disobedience.

"Struggling states," says the State Department's Office of Reconstruction and Stabilization, an important but relatively unpublicized entity that monitors and coordinates the U.S. response to failed and failing states, "can provide breeding grounds for terrorism, crime, trafficking, and humanitarian catastrophes, and can destabilize an entire region."

Among those nations generally regarded as belonging in the category of failed states are the familiar ones: Afghanistan, the Democratic Republic of Congo, Somalia, and Sudan. Countries such as Bosnia in the Balkans and several nations in Africa (Angola, Burundi, Ivory Coast, Liberia, Sierra Leone, and Zimbabwe) are considered by many to be *failing* states – i.e., countries whose central governments are losing their hold on power and/or territory. Other reckonings would flag Colombia, whose otherwise strong central government does not control all of its national territory, as well as Pakistan, Georgia, Albania, Yemen, Nigeria, and Indonesia.

Twelve Indicators and Two Billion People

Last year, the Carnegie Endowment for International Peace, the independent research organization Fund for Peace, and *Foreign Policy* magazine studied the makeup and characteristics of failed states. They arrived at twelve indicators common to failed or failing states and developed a list of sixty such states ranked in order of their vulnerability to violent internal conflict. *[For a comprehensive discussion of this first annual "Failed State Index" visit the link provided at the DomPrep.com website.]*

The Failed-State study calculated that perhaps two billion people worldwide live in failed or failing states, which are characterized by a host of social, political, and economic problems ranging from armed conflict, widespread lawlessness, and human rights violations to famine, disease, environmental degradation, and massive refugee movements and other population displacements. In addition to possessing weakened central governments, failed or failing states that have been de-legitimized, or even criminalized, may be home to competing politico-economic entities – e.g., warlords, drug cartels, paramilitary political opposition parties, ethnic nationalists, and dictatorial clergy – all of whom demand political allegiance. These same states may also, willingly or unwillingly, provide sanctuary to terrorist networks.

In today's increasingly dangerous world, it is obvious that failed and failing states should be on many other radar screens in addition to those monitored by diplomats and the military. If former DCI Woolsey is correct, local LE agencies should develop an increased awareness of international problems that might well affect their home communities, for what goes on today in Nigeria, Colombia, and Afghanistan may have relevance tomorrow on the front lines of homeland security – in the apartment above a local Laundromat, for example, where a node or cell for a globalized non-state cartel or criminal network (whether its stock in trade is drugs or terrorism) may be operating.

"We face a foe more dangerous than a traditional nation-state," writes former CIA officer Michael Scheuer – as "Anonymous" – in his *Imperial Hubris*, "because it has a nation-state's goals and resources, draws manpower from a 1.3 billion-person pool, has no fixed address to attack, and fights for a cause in which death while killing enemies earns paradise."

An Outdated Paradigm, A Foundation of Violence

Scheuer and a number of other respected authors – e.g., Marine Col. Thomas X. Hammes, retired Army Lt. Col. Ralph Peters, and economist Loretta Napoleoni (who has written knowledgeably about the financing of terrorist networks) – are defining new ways of seeing, and thinking, that remove the blinkers that have hampered those whose vision has been focused primarily if not exclusively on either the domestic or the international, but not both. Homeland-security solutions, including those in the intelligence I&W category, are "360-degree," as Hammes would put it.

These same authors argue persuasively for moving beyond the outdated "territorial nation state" paradigm when assessing enemies – and perhaps the United States itself – in order to respond more effectively to the terrorist threat and eventually prevail. Napoleoni uses the term "state-shells" – undemocratic and hierarchical transnational corporations (TNCs) built on a foundation of violence and the monopoly of economic resources within the ungoverned or lawless territories of failed or failing states.

For his part, Hammes says that today's globalized political-economic actors are "idea-based" (as opposed to territorial-based) networks – the members of which may feel they have legitimate grievances, but that have only loose communications between and among their cells. "The world [individuals, groups, businesses, nations]," says Hammes, "is organizing into webs for political, economic, social, and even technical purposes." His point is to state a fact rather than declare outright whether the actor is necessarily good or bad.

Nonetheless, when a terrorist network, operating from its haven in a failed or failing state, conducts operations within the United States (or any other country), it is engaged in warfare in ways unlike those that would be used by its host state or by any traditional territorial nation-state. The non-state terrorist network does not have to honor obligations with any alliances, and is not politically accountable. Because it has no conventional army in the field, it requires neither significant assets nor logistical capabilities. It can, and does in fact, use everyday materials such as those readily available throughout the U.S. economy that have the potential of being shaped into weapons of mass destruction (WMDs).

This potential has profound implications for risk assessment, border protection, and local law-enforcement agencies. It seems reasonable to ask why a cell should or would risk compromising an operation by smuggling chemical/biological/radiological/nuclear/explosive materials into a U.S. port or across a border when it can instead, more easily and with less risk, steal "pre-positioned" industrial materials to fabricate into a WMD.

The Multi-Generational Threat

For some time, the Marine Corps has been calling warfare in the post-Cold War era "fourth-generation" – because it is not about the traditional taking and defending of territory, and governing conquered peoples. "Fourth-generation warfare," Hammes has written, "is about sending messages to decision makers – usually via the mass of people that supports them."

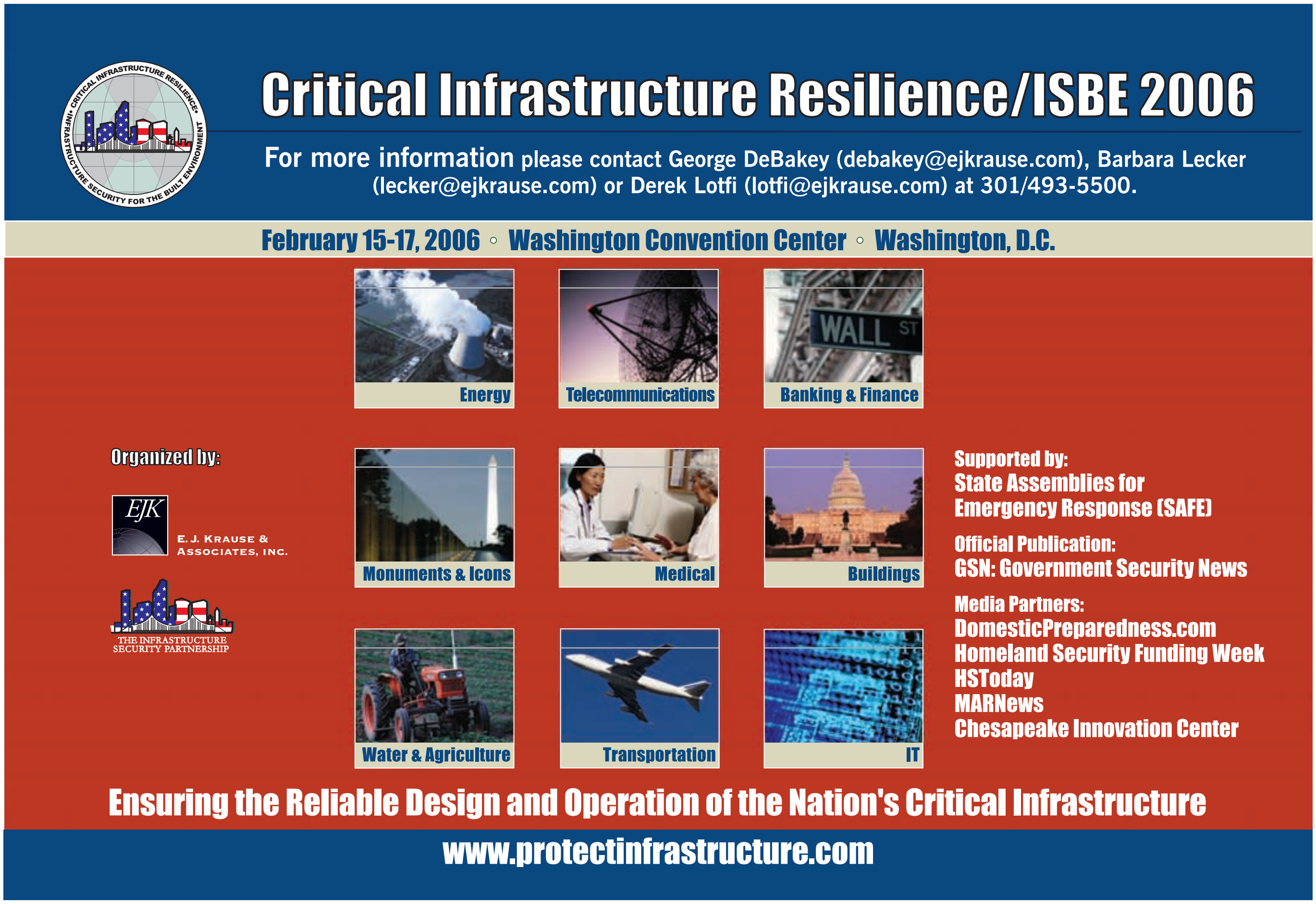
More ominously, Hammes has taken a new look at the 2001 anthrax bio-attacks, and calls them an example of "fifth-generation warfare" – by his definition, an operation conducted by a small group of people, perhaps by only one individual. The impact on government of the 2001 attacks was tectonic, forcing an almost complete closedown of all legislative-branch operations and the U.S. Capitol itself, the ultimate symbol of representative democracy. With those attacks, possibly carried out by only one person, a grim message was successfully sent to U.S. decision makers. The lesson learned from that incident has surely been studied by more than one global malcontent.

Intel used to be focused primarily on assessing an enemy's capabilities through the counting of tanks, ships, and planes. If Hammes is correct in his judgment that the clever terrorist of the future is going to use materials that are already pre-positioned, local law-enforcement agencies may find themselves the driving force in gathering intelligence and sharing information – and, as a corollary, having to rely heavily on their own creativity and resources for the development of future indications and warnings.

Arguably, local LE agencies may have to extend their current graphical-analysis tools to include data from failed and failing states that could be used to determine patterns, trends, associations, and other information that may have relevance to the fighting of terrorism within their own jurisdictions and indeed the nation.

As for the Ghanaians living over the Laundromat, the analysis provided by the criminal intelligence section at police headquarters precipitated a quick decision on resource allocation:

"The presence of Nigerians might have generated significant interest, given that Nigeria is beginning to fail as a state and is notorious for its criminal networks operating worldwide. The comparatively stable Ghana, however, is not found on any list of failed or failing states. … [For that reason], the department is advised not to expend resources beyond any routine follow-up (e.g., checks on immigration status) unduly on any follow-up to this tip."



Spotlight: Homeland Security Activities Far East

Two Important New Components of National Security

By Christopher Doane and Joseph DiRenzo III, Coast Guard

The terrorist attacks on the U.S. Navy's guided-missile destroyer USS Cole in October 2002 and, later, the French tanker Linberg awakened the world to the asymmetric maritime threat posed by terrorist organizations not only to the United States itself but also to other free nations. Responding to the challenges posed by Al Qaeda and other terrorist groups, maritime security forces of countries both large and small have been struggling ever since to find the appropriate mix of laws and regulations, physical security upgrades, operational tactics, and interoperability capabilities needed to cope with the formidable new dangers facing their naval and merchant fleets – their port and maritime infrastructures as well.

The continuing struggle for maritime security has been particularly important in the Far East – for a number of reasons, including the following:

- More than 50 percent of all of the world's merchant shipping is controlled from Asia.
- More than 90 percent of the merchant ships entering or departing from U.S. ports are foreign-flag vessels.
- South Korea is now the largest shipbuilding country in the world.
- China's maritime economy is the fastest growing in the world.
- Singapore and Hong Kong are the two busiest ports in the world.

Considering these facts, and other relevant data that might be cited, it is not surprising that the U.S. Department of Homeland Security (DHS) now maintains a significant presence in the Far East – primarily through two of its most important agencies, the U.S. Coast Guard and the Customs and Border Patrol (CBP) directorate.

FESEC, FEACT, and MIDET

More than 90% of merchant ships entering/departing U.S. ports are foreign-flag vessels

The Coast Guard presence in the Far East dates back to 1947, when Captain Frank Meals, USCG, helped General of the Army Douglas MacArthur form Japan's new Maritime Safety Agency (which was modeled after the U.S. Coast Guard). In 1952, the Coast Guard established its own Far East Section (FESEC) in Japan, at Yokota Air Base, to oversee the operation of its long-range radio aids to navigation (LORAN) systems positioned throughout the Western Pacific and East Asia. In December 1994, FESEC was decommissioned, and a new Coast Guard command – Activities Far East/Marine Inspection Office Asia (FEACT) – was commissioned.

FEACT also became the parent command of the service's Marine Inspection Detachment (MIDET) headquartered in Singapore. Operating under the direction of the Fourteenth Coast Guard District, headquartered in Hawaii, FEACT operates in and throughout a huge geographic area of responsibility encompassing 41 independent nations and tens of thousands of square miles of international waters.

FEACT personnel are assigned numerous responsibilities, including the conduct of safety inspections aboard both U.S.-flag and foreign-flag commercial ships – always, of course, in accordance with U.S. law and various international agreements to which the United States is a signatory. Having an important Coast Guard presence in the Far East not only helps the service carry out its Marine Inspection responsibilities, it also provides an excellent opportunity for building friendly relations with foreign maritime agencies throughout the Far East.

Improved Security and An Escalating Confidence

The value of these always important relationships escalated significantly in 2004 when the Coast Guard launched an International Port Security Program to comply with new cargo and shipping requirements mandated by the U.S. Maritime Transportation Security Act of 2002 (MTSA) and the International Ship and Port Facility Security (ISPS) Code.

The principal purpose of the new international program is to establish and maintain a dialogue between maritime nations on ways to improve port and maritime security, share best security practices and security concerns, and observe one another's port security operations (to build confidence in the adequacy of the security measures implemented by America's trading partners). As the first step in the program, the Coast Guard assigned International Port Security Liaison Officers to various offices in the United States and Europe, and to both FEACT and MIDET.

Building upon the friendly international relationships already created throughout the Far East by FEACT, the liaison officers assigned to that area have been able to develop even stronger ties with maritime officials and industry leaders throughout the Far East. This has resulted in an active sharing of security practices and concerns during visits by U.S. security personnel to Far East ports, and during reciprocal visits to U.S. ports by security personnel from Far East nations. Among the list of countries visited by the new Coast Guard liaison teams are China, Indonesia, Japan, Singapore, and South Korea.

Several Ounces of Preliminary Prevention

CBP also is working closely with several countries in the Far East to implement the new U.S. Container Security Initiative (CSI), a DHS program initiated in 2002 that has already significantly improved the security of maritime shipping containers. The CSI program, which is designed to screen containers at designated international ports – again, always with the cooperation of the host country – before the containers are loaded on U.S.-bound ships, assigns CBP agents to work side by side "in country" with the host nation's security personnel.

The key components of the CSI program, as posted on the CBP web site, are: (a) The use of intelligence and automated information to identify and target containers that pose a potential risk of terrorism; (b) The *pre-screening* of those containers *at the port of departure* – i.e., long before they arrive at U.S. ports; (c) The development, production, and use of advanced detection technology to pre-screen containers that pose a risk just as quickly as possible; and (d) The increased use of "smarter" tamper-evident containers.

A secure container transportation and delivery system is obviously a critical component of the "just in time" inventory-management system used by industries throughout the world. According to a 22 September 2004 report released by the Congressional Research Service, containers now "account for 90 percent of all world cargo" and approximately seven million "are offloaded in U.S. seaports annually."

The Hidden Trillion-Dollar Price Tag

There is an even more important factor to be considered – namely, that the effects of a successful terrorist attack through the use of a weapon of mass destruction hidden within a container not only could be devastating to the U.S. economy but also could result in thousands of casualties. In fact, according to a 2002 Brookings Institution report – *Protecting the American Homeland: A Preliminary Analysis* – written by a team led by Dr. Michael E. O'Hanlon (senior fellow for Foreign Policy Studies), a successful attack could cost the United States as

much as one trillion dollars, a total that dramatically illustrates the high stakes involved in the effort to improve the nation's port and maritime security.

The ports currently partnering with CBP on the CSI initiative within Asia and the Far East include not only Hong Kong and Singapore but also Yokohama, Tokyo, Nagoya, and Kobe, all in Japan; South Korea's Pusan; Malaysia's Port Klang and Tanjung; Thailand's Laem Chabang; and China's Shenzhen and Shanghai. CBP agents also can make formal requests to other host-nation personnel to carry out examinations of high-risk containers before they are loaded aboard U.S.-bound ships. All evidence suggests that the new security partnerships are working well.

In fact, the combined international efforts of the CBP and U.S. Coast Guard seemed to be making a big and beneficial difference. But the threat posed by maritime terrorists keeps adapting – and growing – so the world's security forces must continue to adjust, especially in the Far East where the stakes are so high.

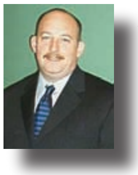
Christopher W. (Chris) Doane is the Coast Guard Atlantic Area's Chief of Response and Port Security. He completed a 21-year Coast Guard career in 2003 as a commander whose career spanned a variety of programs from surface operations to shore operations to readiness and marine safety and security.

Joseph DiRenzo III is the Coast Guard Atlantic Area's Anti-Terrorism Coordinator, responsible for inter-agency, especially DoD coordination, for all Ports, Waterways and Coastal Security (PWCS) events and operations. He also serves as the primary liaison to the Anti-Terrorism staffs at Navy Fleet Forces Command, Commander, Second Fleet, and Submarine Force Atlantic. DiRenzo, is a retired Coast Guard officer, who spent nine years in the Navy, in both the submarine and surface warfare communities qualifying in both specialties.

Both are retired Coast Guard Officers and have written extensively on port and maritime homeland-security issues for the national and international media.

What Is an Ambulance?

By Joseph Cahill, EMS



As the foundation of a workable national structure that will meet emergency-response requirements, the Department of Homeland Security (DHS) created and is relying on two major documents – one describing the National Incident Management System (NIMS), the other establishing a National Response Plan (NRP). Within the latter, EMS (emergency medical services) falls firmly under ESF-8 – Emergency Support Function (Health and Medical Services) – and plays a vital role in the nation's medical system.

Nationally, EMS is now provided by an amalgam of government agencies, volunteer organizations, hospitals, and private companies. This patchwork semi-organization is a residue of decades of non-inclusion of EMS units in disaster-preparedness plans and the decades-long reliance, by many cities and states, on private resources to provide emergency medical services.

Modern EMS can trace its roots back to concepts developed for the civilian community in the 1950s that were based on the lessons learned in combat during World War II and later upgraded and refined in the Korean War. The doctrinal genesis of modern EMS, however, lies in the 1966 publication by the National Highway Transportation Safety Administration (NHTSA) of a White Paper titled "Accidental Death and Disability: The Neglected Disease of Modern Society."

Two Strong Men And a Station Wagon

The NHTSA document precipitated the transformation of ambulance services from little more than two strong men in a station wagon to the modern model in which effective medical care is provided both at the scene of a life-threatening accident or disaster and en route to the hospital. Prior to this change, about half of all ambulances in the United States were run by mortuaries (primarily because their vehicles were big enough to carry at least one stretcher patient).

Accompanying the shift to a more professional, medically grounded EMS was the growth of ambulance transportation as a business. After ambulance companies were able to bill Medicare/Medicaid and/or medical-insurance companies for their services there was a virtual explosion in the number of ambulance businesses and operators available. That unprecedented and somewhat unregulated growth eventually was brought under control in many states by a certificate-of-need process that requires the demonstration of a need prior to the authorization of any individual or business to operate an ambulance service.

125 of the nation's 200 largest cities rely on the private sector to provide some if not all critical emergency services

In recent years, many communities have been either consolidating their EMS services into their police or fire departments, or privatizing their EMS systems. One unfortunate result, though, has been a lack of consistency in regard to the type and structure of EMS resources and capabilities available nationally. Although fiscal realities may have forced these changes, the bottom line, according to a 2004 survey by the *Journal of Emergency Medical Services*, is that about 125 of the nation's 200 largest cities now rely on the private sector to provide at least some if not all of the critical emergency services needed in those cities.

Resource typing allows incident commanders to request what they need and expect a minimum level of consistency regardless of source

A Partial Solution Under NIMS

One of the more important questions facing local and state officials is how to ensure that private-sector ambulances are fitted with the same types and quantities of equipment available to those of their municipal counterparts, and that private-sector EMS personnel possess a level of training equivalent to that required for city, state, and federal EMS employees. Experience has shown that the vast majority of EMS personnel working in for-profit ambulance companies *are*, in fact, highly trained and dedicated professionals. However, as private businesses the companies that employ these skilled workers often are not eligible for the same grants and other publicly funded programs available to the EMS professionals themselves.

Similarly, agencies that rely on *volunteers* for staffing often have trouble motivating them to take any but the absolute minimum training – primarily, it seems, because most if not quite all volunteers not only are donating their time but also are putting in a full day's work in their other jobs.

The NIMS plan provides at least a partial solution to this problem. Although *no* incident-management system will correct the economic and historical disparities that have led the nation's EMS resources to the current state of semi-confusion, NIMS can and does help level the playing field on the day an actual incident occurs. One of the more important issues addressed by the NIMS guidelines is resource management. As already has been demonstrated in certain incidents that reached the level of "National Significance," the control of resources is the key to success in responding to almost any emergency.

A principal focus of resource management under NIMS is resource typing – or, more simply put, the categorizing of similar resources by capability. The first step to understanding resource typing in EMS is to recognize that, although there are a number of state-to-state variations in other particulars, most ambulances can be categorized as either BLS (basic life support) or ALS (advanced life support) vehicles. The equipment and (to a somewhat lesser extent) personnel specifications for each category of vehicle can easily be spelled out, thus eliminating at least some previous uncertainties.

Consistency Requirements And the EMAC Solution

When resources are needed during an incident they usually are drawn, initially, from the community where the emergency occurs. This means that there is not only a consistency of resources but also that those requesting and those providing the resources both understand and expect the same consistency. Resource typing is intended to ensure that the consistency continues if and when the need to respond to a major incident requires using other resources drawn from other, usually more distant, jurisdictions.

Resource typing allows incident commanders not only to request what they need but also to expect a minimum level of consistency regardless of the source. A simple example would be an incident commander requesting an ALS unit. If resource typing was in place beforehand the request might be for a type-I ALS ambulance. Because the providing agency had previously agreed on what a type-I ALS unit is, the result will or should be a consistent resource. (In the case postulated, that resource would be a paramedic unit that can transport two patients and that possesses a specific set of equipment, as well as EMS personnel with the training specified.)

This consistency requirement carries through the other types of EMS units. The collective state/local/federal EMS goal is to develop and use a common vocabulary so that both the requesting agency and the providing agency know and agree, in specific detail, what is being requested and what is being provided. Nonetheless, it still happens that, when one town is requesting a resource from a neighboring town in the same geographic community, the definition of the resource is often not understood – unless there has previous discussion between the two towns. When the towns are adjacent to one another this usually is not a problem, because the same rules almost always apply to both towns. However, this expectation becomes less and less certain as the distance between the requester and the provider grows.

Emergency Management Assistance Compacts (EMACs) – i.e., state-to-state mutual-aid agreements – allow states to request assistance from and/or lend assistance to other states in the same area of the country. Having a common language to describe the resources requested will allow the fulfillment of EMAC requests not only to be more meaningful – and, therefore, both more productive and more effective – but also lead to the saving of additional lives.

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 situations 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
800.638.8093

Cyber Attacks: The Need for Resiliency

By Thomas Kellerman, Cyber Security

The U.S. continuity-of-operations movement, intended to ensure that businesses as well as offices and agencies at all levels of government – non-government organizations as well – has changed significantly since 9/11, and seems likely to change even more in the foreseeable future.

Continuity-of-operations planning, which concentrates primarily on consequence management and recovery from all types of disaster, both natural and manmade, is not a new concept. However, prior to 9/11, the planning focused on reacting to localized disasters or failures – i.e., protecting the bricks-and-mortar aspects of operations. Since 9/11, the continuity of operations has become increasingly dependent upon technology, and it is this technology that now poses a major risk to operations, which in recent years have become more and more digitized. What were once legacy systems are now connected to the Internet, and cyberspace itself has become a hostile environment.

FBI, World Bank, and DHS (Department of Homeland Security) studies have all documented an exponential growth in cyber attacks in recent years. In 2002, FBI Director Robert Mueller said that fighting cyber crime had become his "Number One" priority. Additional evidence of the continuing growth in cyber crime was provided by the 2005 E-crime Watch Survey – carried out by the U.S. Secret Service and the Carnegie Mellon CERT Coordination Center – which reported that 68 percent of those responding to the survey had experienced at least one electronic security incident, and that the average number of electronic crimes or intrusions experienced by the organizations surveyed was 86 events. According to the same survey, "outsiders" – i.e., perpetrators who were not members of the organization(s) per se – had committed an estimated 80 percent of the electronic crimes reported.

The fact that so much espionage, sabotage, and other crimes now occur in the virtual world is clear evidence that today's hackers possess an ever-growing ability to harness the technological capabilities of powerful and evolutionary malicious code. That ability permits the hackers to become "digital insiders" who, once inside a compromised system, can use these malicious pieces of code to act both autonomously and stealthily, frequently if not always escaping the notice of an organization's security controls.

Responding to Cyber Security Incidents

In large part because of the growth in cyber crime that has been documented, the ability of an organization to react both quickly and effectively to security incidents has becoming an increasingly essential component of an overall security plan. An organization's continuity of operations depends on its ability to provide timely information to its staff in the form of electronic data. If that ability is crippled or compromised, the organization's continuity of operations cannot be guaranteed.

An incident response plan (IRP) is the primary document most organizations use to establish how they will identify, respond to, correct, and recover from computer security incidents. Whatever the plan is called, though, all organizations of any size should have comprehensive IRPs in place, and should test them periodically. Moreover, all employees of an organization should be trained in the correct procedures to follow in the event of a computer incident. Following are some guidelines to follow in the development and promulgation of an effective incident response plan:

1. The organization's security, legal, and public relations departments all should participate in the development and implementation of the organization's incident response policy.
2. All of the incident-response agencies responsible for the security of an organization's site should be contacted when a security incident has been determined (or is suspected). Among the more important of those agencies are the National Infrastructure Protection Center, the Computer Emergency Response Team, European Computer Emergency Response Teams, the Electronic Crimes Taskforce, and the Forum of Incident Response Security Teams.
3. Out-of-band methods (phone calls, for example) should be used for communications when an incident has been detected, or is suspected, to ensure that intruders do not intercept information they do not already have. Arguably, this is the most important element of the IRP, because it identifies certain situations or conditions and postulates in detail how to respond to those situations or conditions. The term incident notification describes the procedures to be used in notifying the computer user population when an incident has been confirmed. For that reason, this section of the plan clearly identifies those who must be notified in the event of an incident, and also provides the critical contact information required and the contact procedures that should be followed.

A Flood of Information – Or a Trickle

During a natural or "physical" disaster – hurricanes, earthquakes, floods, and tornadoes, for example – a massive amount of information usually is provided to the general public through a variety of sources, including media reports and public statements by government agencies.

However, when a business or other organization experiences a cyber event, the information available to it is generally limited to whatever that organization or business has found out on its own. For that reason alone, effective proactive planning and timely responses are significantly improved when an organization is able to understand both the types of attacks that are possible, and how to defend against them.

Individual users also can greatly enhance the reaction of an organization to a cyber attack. Basically, if a computer is believed not to be operating normally, the individual user should immediately disconnect the computer from the Internet and from all wireless access points. Any or all of the following should be considered suspicious behavior: The computer is operating slowly; it will not allow the user to close a given window; the computer screen is blue; and/or the computer seems to be running multiple programs that were not previously running.

The next step should be to call the IT specialist, through a landline, to notify him or her of the suspected incident. If an IT specialist cannot be found the individual user not only should follow the procedures spelled out in the organization's IRP but also consider the following additional actions: (a) Isolate the virus scanner, then start a full scan on the C: drive; (b) Update all critical software patches; (c) Delete temporary files; and (d) Change his/her password and advise all other employees to do the same.

When a website or network has been compromised, one of the remediation techniques some organizations use is to restore from backup. But when an organization has no way to determine when the site was compromised, it cannot accurately determine when the last acceptable backup had been collected. In these circumstances, a "restore + patch" procedure might seem to be a logical move, but that might simply restore the backdoor Trojan or malware to its previous state. In most organizations the backup systems already in place could regenerate yesterday's threats if not properly audited and cleaned for malicious code. The most important point to remember is that effective incident response is the paramount consideration in the battle to clean and preserve classified data.

If nothing else, the 9/11 terrorist attacks should have taught Americans not to underestimate the sophistication and resolve of this nation's enemies – whose capacity to use technology against the United States is still growing. This is a grim fact of modern life that should be recognized, and acted upon, by all agencies and organizations charged with the creation and promulgation of timely and effective incident response plans.

Thomas Kellerman is the Chief Knowledge Officer & CoFounder of Cybrinth LLC. He serves as a member of the New York Chapter of Infragard, the New York Electronic Crimes Taskforce and the Department of Homeland Security US-CERT Emerging Threats Working Group.

Connecticut, Tennessee, and Texas

By Adam McLaughlin, State Homeland News

Connecticut Designs New Device to Solve Communication Woes

Connecticut emergency responders believe they have developed a unique communications device that will allow responders from different agencies and jurisdictions to talk to one another at the scene of an emergency or disaster. If the invention proves to be successful, it would help clear one of the largest hurdles that homeland-security officials have been attempting to negotiate since the 2001 terrorist attacks: the inability to communicate across radio frequencies.

The device has been named STOC, which stands for on-Scene Tactical Operations Channel. STOC combines a radio and receiver into a single box that instantly receives a signal from one frequency and sends it onto another frequency. The system was developed by a state communications workgroup led by Michael Varney, the fire chief of Ellington.

"A prototype has been developed, another is in the works, and state officials have allocated nearly $2.1 million to build a new box for towns across the state," said Wayne Sandford, the state's homeland-security deputy director. Sandford said he believes that Connecticut is the first state in the nation to develop such technology. He added that the communications workgroup should know within a few months if STOC is successful.

Tennessee Sumner County Prepares for Future Disasters

The Sumner County Emergency Management Agency hosted a major 9/11 tabletop exercise earlier this month at the county's emergency operations center in Gallatin that is expected to help all jurisdictions – local, state, and federal – in Tennessee cope more effectively with future disasters, both natural and manmade. Participants in the exercise included representatives from the Sumner County police and fire departments, the Tennessee Valley Authority, the Federal Bureau of Investigation, the Tennessee Emergency Management Agency, and the Federal Emergency Management Agency.

The scenario for the exercise centered on a simulated terrorist attack on the Tennessee Valley Authority power generation plant in Gallatin. The overall goals of the exercise were to improve the participants' understanding of response plans, identify opportunities and/or problems with current plans, and develop a spirit of cooperation and support within and between all of the agencies involved. On the operational level, the objectives were to improve inter-agency planning and coordination, discuss the need for resource coordination, promote the understanding of various threat/hazard-related issues, and consider the options available for providing timely information to the public and media.

"I believe everyone involved benefited from learning their roles in Sumner County's emergency management plan," said Kenneth Weidner, director of Sumner County emergency management. "They also learned the importance of a county-wide communications system and the need for interoperability among our own agencies as well as with neighboring counties.

"The tabletop exercise allowed us to test our responses and capabilities should Sumner County face a natural or man-made disaster," he added. "I am proud to assure you that we have emergency management plans in place that will serve our citizens safely and efficiently."

Texas Beaumont Leaders Use Rita Template for Future Disasters

City and county leaders from the Beaumont area have been closely studying the lessons learned during Hurricane Rita, and in the weeks and months that followed, and developed a plan earlier this month to deal more effectively with the next disaster.

A broad range of issues – including what went right and wrong, the staffing levels required for emergency operations centers, communications requirements, body storage for the dead, and the need for pre-planned shelters and evacuation centers – were on the table at a meeting at the Ford Park Exhibit Hall. "We already have a plan, and this will assist us in updating and refining the plan," said Judge Carl Griffith of Jefferson County. "These lessons learned [during the Ford Park meeting] will be incorporated and used wisely."

Mayor Joseph Hopkins of Vidor said that most of the problems his city faced in the wake of the storm involved the distribution of scarce resources such as fuel, food, and generators. He suggested that a single organization be assigned the job of allocating and distributing resources after disasters. "I think it would be great if the state did that, instead of ... [first responders and the citizens affected] having to call 200 or 300 different entities," Hopkins said.