

Community Response to the Threat of Terrorism

**Issues and Ideas Papers
Presented During a
PERI Internet Symposium**

Presented November 2001

Published by the Public Entity Risk Institute
On the Web at: www.riskinstitute.org

This material is provided free of charge, as a public service of the Public Entity Risk Institute (PERI), 11350 Random Hills Rd., Suite 210, Fairfax, VA 22030. Phone (703) 352-1846. Web: www.riskinstitute.org.

The Public Entity Risk Institute (PERI) provides these materials “as is,” for educational and informational purposes only, and without representation, guarantee or warranty of any kind, express or implied, including any warranty relating to the accuracy, reliability, completeness, currency or usefulness of the content of this material. Publication and distribution of this material is not an endorsement by PERI, its officers, directors or employees of any opinions, conclusions or recommendations contained herein. PERI will not be liable for any claims for damages of any kind based upon errors, omissions or other inaccuracies in the information or material contained on these pages. PERI is not engaged in rendering professional services of any kind, and the information in these materials should not be construed as professional advice. Users bear complete responsibility for any reliance on this material, and should contact a competent professional familiar with their particular factual situation if expert assistance is required.

Community Response to the Threat of Terrorism

**Issues and Ideas Papers
Presented During a
PERI Internet Symposium**

Presented November 2001

Published by the Public Entity Risk Institute

11350 Random Hills Road, Suite 210
Fairfax, VA 22030

Phone: (703) 352-1846 FAX: (703) 352-6339

On the Web at: www.riskinstitute.org

Public Entity Risk Institute

The Public Entity Risk Institute's mission is to serve public, private, and nonprofit organizations as a dynamic, forward thinking resource for the practical enhancement of risk management. PERI pursues its mission by:

- Facilitating the development and delivery of education and training on all aspects of risk management, particularly for public entities, small nonprofit organizations, and small businesses.
- Serving as a resource center and clearinghouse for risk management, environmental liability management, and disaster management information.
- Operating an innovative, forward-looking grant and research program in risk management, environmental liability management, and disaster management.

For complete information on PERI's programs and information services, visit our Web site at www.riskinstitute.org.

To access a wealth of risk management intelligence, please visit the Risk Management Resource Center, at www.eriskcenter.org, a collaborative Web site operated by PERI, the Public Risk Management Association (PRIMA), and the Nonprofit Risk Management Center (NRMC).

Public Entity Risk Institute
11350 Random Hills Road, Suite 210
Fairfax, VA 22030
Phone: (703) 352-1846
FAX: (703) 352-6339

Gerard J. Hoetmer
Executive Director
(ghoetmer@riskinstitute.org)

Claire Lee Reiss, J.D., ARM
Director, Grant and Research Program
(creiss@riskinstitute.org)

Dennis Kouba
Director, Outreach and Development
(dkouba@riskinstitute.org)

Audre Hoffman
Office Manager
(ahoffman@riskinstitute.org)

Table of Contents

About PERI's Symposium Programs	vi
Introduction and Overview: Community Response to the Threat of Terrorism	1
The Incident Command System and the Concept of Unified Command at a Terrorist Incident	9
Public Works and Terrorism	17
Chemical and Biological Terrorism	23
Fire Departments, Emergency Medical Services, and Emergency Management Agencies	35
Emergency Medical Response to Terrorist Incidents and Hoaxes	39
The Challenge of Cyberterrorism	49

About PERI's Internet Symposium Programs

These Issues and Ideas Papers were presented during one of PERI's "virtual" Symposium Programs, programs that are conducted entirely via the Internet. Community Response to the Threat of Terrorism was presented in November 2001.

This publication is also available electronically on PERI's Web site at www.riskinstitute.org and on the Risk Management Resource Center at www.eriskcenter.org.

How We Conduct a Symposium

Our programs consist of specially commissioned papers, and an open, threaded discussion. Participation in the discussion is free and open to anyone interested in the subject of the Symposium.

Each day during a PERI Symposium, we present an Issues and Ideas Paper (or Papers) written by recognized experts. Each paper addresses a different aspect of the subject of the Symposium.

The papers are intended to be thought-provoking -- raising risk management issues about the week's subject -- and practical -- offering useful ideas and solutions.

Papers are posted each morning of the Symposium for reading. We also send the papers via e-mail each morning to participants who sign up ahead of time.

The discussion portion of the Symposium is a threaded discussion, in which comments and replies are posted in our Symposium Center, and are accessible by all. Anyone can view or post comments.

Our Symposium Programs are an important way for us to meet our goal of facilitating the delivery of education and training on all aspects of risk management. Participation in the programs is free and open to anyone interested in the subject.

Future Programs

For the schedule and topic of future programs, please visit PERI's Web Site at www.riskinstitute.org.

Introduction and Overview: Community Response to the Threat of Terrorism

**By Lawrence J. Hogan
Symposium Moderator**

Welcome to the Public Entity Risk Institute Symposium, *Community Response to the Threat of Terrorism*.

The Issues and Ideas Papers that will be presented over the next week will provide you, we hope, with thoughtful, practical, and valuable ideas on what to do to prepare your community against the threat of a terrorist act. We encourage you to circulate the papers to others in your organization.

We especially encourage you to offer your thoughts in the open discussion that is such a vital part of this Symposium. The value of the program will increase exponentially the more you participate. I urge you to share your thoughts and viewpoints, and to ask and answer questions – like most conferences we attend, some of the best and most helpful ideas will come from your colleagues.

Please “speak up” from your computer keyboard. To join in the discussion, go to the “Current Program” section of the Symposium Center on PERI’s Web site – www.riskinstitute.org. It’s easy to participate.

Ask questions or make comments about the topics covered by the presentations. The experts who authored the papers will be standing by to respond to your input.

Over the next few days, we will address different aspects of a community’s preparation and response.

Overview

Terrorism is a multi-faceted problem: It’s a police problem, a military problem, a public safety problem, a political problem, and a public policy problem.

As we have learned, international terrorist groups have a support infrastructure within the United States, giving them the capability to attack us virtually anywhere they choose any time they choose. In a free country such as ours, it is easy for terrorists to operate and extremely difficult to cope with them. There is rarely a terrorism event which affects only one area.

In addition to international terrorists, we also need to be concerned about white supremacist, anti-government military groups, environmental terrorists, and free lancers -- all present special problems for governments at all levels.

Local government policy makers should authorize police agencies to monitor the activities of these terrorist groups in an effort to get advance warning so they can thwart potential terrorist acts.

Will these organizations be investigated? Will they be infiltrated with informants? Kept under surveillance? These questions have civil liberties' overtones and could become politically embarrassing for the local government and its policy makers. However, having a terrorist incident that might have been prevented by sound intelligence information would be more than just embarrassing. In counter-intelligence activities, success is measured by what DOES NOT HAPPEN !

The basic purpose of government is to protect lives and property. Everything else springs from that fundamental duty.

Regarding terrorism, government has a two-fold mission:

- PREVENTION -- Intelligence gathering.
- REACTION -- Responding to and investigation acts committed by terrorists.

Keep uppermost in mind that when a terrorist incident happens, the local first responders will be first on the scene. Federal personnel may not arrive for several hours. Acts of terrorism, like all crimes, are primarily local. Recognizing that fact, the federal government is committing a considerable amount of money to train and assist local governments in this effort.

Because state and local governments are charged with the primary enforcement and public safety responsibilities related to terrorist attacks, there must be a close working relationship between a local government's policy makers and operational people and with other government agencies at all levels.

In addition to other international terrorists, you may have in your area American organizations which have strong ethnic or nationalistic ties to foreign countries and these groups might pose a terrorist threat. Strong and bitter rivalries between nations or ethnic and religious groups within other nations are frequently reflected in sympathetic U.S.-based organizations. These domestic groups might be made up of former nationals of those countries and their descendants or American citizens with shared cultural, religious or ideological affinity, or foreign students.

Visits by foreign dignitaries might also pose a danger. Assassinations, bombings, kidnapping, and other acts of violence against official or unofficial representatives of the rival country or group while visiting the United State constitute serious terrorist problems, even though the United States itself might not be the target of the hostility in those instances. But, if it happens here, it's our problem.

There is a need to develop a cooperative partnership among local, state, and federal law enforcement agencies and other emergency response agencies along with a coordinated incident command system. (John Kane will discuss this in his presentation.)

What Should You Be Doing Now?

What should local governments be doing in the face of these multiple threats?

First of all, make sure your emergency operating plan includes an up-to-date annex on terrorism, convene your top people to revise this plan to assess your vulnerabilities and capabilities with respect to terrorism, and study the problem as it specifically relates to your community.

- Where are you vulnerable?
- What events are planned for your area which might be tempting targets for terrorists: Sports events or tournaments, political conventions, world fairs, World Trade and International Monetary Fund meetings, etc.?
- What visits by VIPs or foreign dignitaries are scheduled in your area which might tempt terrorists?

What facilities might be targets? Airports, hospitals, bridges, tunnels, military bases, amusement parks, water supply facilities, dams, government facilities, electric power plants, transmission lines for oil and gas, theaters, conference halls, sports arenas and stadiums, embassies, consulates and other diplomatic facilities -- all are potential targets for terrorists.

What groups or individuals in your specific area pose threats?

What equipment and training do you need to be adequately prepared?

[Congress has directed the Department of Justice to administer a grant program for local first responders to enable them to buy equipment to respond more effectively to a terrorist attack. For more information about these grants, contact the Office of Justice Programs Office for State and Local Domestic Preparedness Support at 202-305-9887. or at www.ojp.usdoj.gov/osldps.]

Do you have the right kind of team in place to cope with a terrorist attack? Are your personnel properly trained? Does this team include:

- Trained hostage negotiators,
- Public information specialists,
- Incident response forces for hostage seizures, bombings and bomb threats,
- Biochemical experts, and
- Cooperative links with other jurisdictions -- police, fire, medical, search-and-rescue etc., under up-to-date mutual aid agreements to share intelligence, training, equipment, and personnel?

Do you have computer experts to monitor the Internet and guard against viruses? Terrorists use the Internet to propagandize, raise money, and recruit new members and to send messages to their “sleepers.” Our computers are very vulnerable to crippling attacks. (Robert Thetford will discuss this in his presentation.)

Have you designated a coordinator to conduct liaison with federal and state authorities?

Do you have employees or outside consultants with the foreign language capabilities you might need? Do you know what foreign language capabilities your employees have? Have you identified university language teachers who might be available to help with translations?

Your plans should also include educating citizens about the potential threats and alerting them to suspicious things to be on the lookout for.

Do you have adequate security at your government buildings and other vulnerable facilities. (Richard Evans covers this in his presentation.)

Do you have a bomb-sniffing dog, an armored personnel carrier and a robot to facilitate safely approaching barricades?

If you don't have these things you should know where you can borrow them.

Have you considered giving inoculations for anthrax and other biological agents to personnel who might be placed at risk? (Dr. Vaughn Wagner covers biochemical threats in his presentation.)

Are your personnel alert for a possible links between terrorism and collateral crimes such as robberies, vehicle and explosives thefts, etc? Terrorist groups often commit robberies, or engage in drug trafficking and other crimes to finance their operations.

What policies should govern a hostage-barricade situation?

What is your policy on the use of deadly force? While you may have an on-going policy on this, circumstances in a specific terrorist incident might require it to be modified.

Elected officials should make sure they appropriate sufficient resources for their operational people to be adequately prepared.

In addition to up-to-date mutual aid agreements with neighboring jurisdictions, local governments should negotiate Memoranda of Agreement with military bases in the area.

Ensuring Continued Government Operations

Make sure your provisions for succession of power are adequately addressed and that the government's essential records are safeguarded -- tax and land records and other documents -- which the government needs to continue operating. There should, of course, be back-up computer files for these essential records.

Ensure that provisions are made to delegate to appropriate officials the authority they need to carry out their duties.

Have you provided for relocation of your seat of government if that should become necessary?

Do you have laws in place to give your top officials the authority to invoke marshal law, rationing, price controls, curfews, anti-hoarding and anti-black marketing programs?

Public Communication and Media Relations

Don't overlook the public relations aspects of the problem. It is important for the government to constantly reassure the citizenry that the government is responding appropriately and to inspire confidence in the government's ability to cope with the problem. It is often desirable for the elected head of the government to appear before the media with the aura of governmental authority to keep the public informed.

You may have a clash with the media in terrorist incidents. It is always a challenge to balance the public's right to know against the government's right to withhold information for public safety. As part of your advance planning, you should discuss this dilemma with the media in your area because policy makers often face very difficult decisions and may be exposed to severe and often unfair criticism from the media, which has the effect of eroding the public's confidence in the government.

Some years ago, Ted Koppel moderated a discussion on the relationship between the American media and international terrorism.

Koppel said to his media guests that finding one of the most wanted men in the world who had promised to murder the President of the United States may be a major journalistic coup, "but when a television network agrees to keep his whereabouts secret, is that journalism or aiding terrorism?"

Tom Brokaw replied that he thought it was journalism. He said NBC decided to keep secret Mohammed Abu Abbas' whereabouts "because we thought the news value outweighed" bringing him to justice. Brokaw said that Abbas had admitted his role in the hijacking the Achille Lauro ocean liner but had "made some very serious charges against the American people and the American president in the wake of the Libyan bombing." (One wonders if Tom Brokaw would feel the same way today if another reporter interviewed the

person who had recently sent the anthrax-laden letter to his office but would not reveal that terrorist's identity or whereabouts.)

The important thing for local government leaders to recognize is that the media do not always see matters the same way government people do and often the media's desire for a story transcends everything else.

Some years ago, a man took over the IBM facility in Montgomery County, Maryland, which resulted in three deaths and injuries to more than 20 people. A news reporter telephoned the IBM building and injected herself into the negotiating process with the perpetrator. Her comments were potentially very inflammatory. There were clearly grave dangers, not only in the manner, but in the content of this interference by the reporter.

That same year there was an incident at the Lake Braddock area in Northern Virginia in which hostages were held for more than 12 hours. A radio station broadcast sensitive information about the hostage taker who was listening to the broadcast! He became very agitated and the hostages were clearly endangered by the radio station's actions. In both the IBM and the Lake Braddock incidents the media alerted the hostage taker to positions and movements of police personnel.

At Waco, when the ATF planned to raid the Davidians' compound, they notified the media. The media, in turn, notified the Davidians. After a 45-minute exchange of gunfire, four ATF agents were dead and 15 were injured.

Remember: you have no obligation to provide information to the media, especially if it might jeopardize your response activities. It is **NOT** a fourth Amendment issue even though the media will claim that it is.

Preparation the Key

At the first anniversary of the Oklahoma City bombing, a memorial was put on display at the federal building. It reads"

We come to remember those who were killed, those who survived and those who were changed forever. May all who leave her know the impact of violence. May this memorial offer comfort, strength, peace, hope and serenity.

New Yorkers are now contemplating what kind of a memorial they should have at the site of the World Trade Center Towers.

Adequate preparation to cope with terrorism might eliminate the need for some future similar memorial in your community.

About the Author

Lawrence Hogan is an adjunct instructor in the Federal Emergency Management Agency's (FEMA) "Consequences of Terrorism" course. He has been developing and teaching courses for FEMA's Emergency Management Institute and the National Fire Academy since 1982. His career in public service includes two years as a member of the Maryland Governor's Commission on Law Enforcement and the Administration of Justice, and six years as a U.S. Congressman from Maryland. From 1978 to 1982 he was the elected County Executive of Prince Georges County, Maryland. He served with the Federal Bureau of Investigation (FBI) for ten years.

* * * * *

The Incident Command System and the Concept of Unified Command at a Terrorist Incident

**By Lt. John Kane
Sacramento, Calif. Police Department**

Preface to the Unified Command Discussion

When I found out that I was going to be addressing an audience as large and as varied as this one today, I wanted to add some remarks to my Unified Command lecture. These remarks are specifically targeted at the managers and local elected officials in the audience:

City managers, county executives, city councilpersons, county supervisors, business managers, security managers, building managers – YOU ARE NOT READY FOR A TERRORIST INCIDENT! And I am hearing that local Chiefs are saying that they are prepared and ready to handle one of these incidents!

To properly handle one of these events at the local level requires a huge amount of coordination, training, and drilling between the key players, and this HAS NOT OCCURRED. I want you to take everything you have heard from your local Fire Chief, Chief of Police, or Sheriff about how well prepared they are, and how much more money they want, and just put it up on the shelf for a few minutes as you read this, especially the questions at the end of this introduction which I want you to ask.

If your job falls into one of the key management or elected positions I have mentioned above, you need to go on your own private fact finding tour, now – and I mean right now. You need to go on your own tour to determine the actual state of readiness in your local area, not what you have been told by the various bosses. They have their own interests to protect. I don't want to get too dramatic, but there are lives at stake, the lives of your co-workers and citizens, so for your own piece of mind I want you to verify what you've been told and make sure your local area is ready to handle one of these events.

I had the pleasure of interviewing California State Senator Nick Petris in the early 1990s for a course on disaster operations I was putting together here in California. Senator Petris' district suffered the Oakland / Berkeley Hills fire of 1991 in which 26 people died and more than 3,000 homes and apartments were destroyed. He investigated this event from the perspective of how it was managed.

His investigation found that each police and fire agency in California had a different protocol or method on how to handle major incidents. They often had different names for similar tasks. The differences in these systems resulted in some confusion and inefficiency in the management of this event as many agencies came together in mutual aid to help fight the fire and rescue people. It was from Senator Petris' investigation, and subsequent groundbreaking legislation, that California enacted the Standardized

Emergency Management System (SEMS). This system mandates that we all utilize the same management framework as we manage critical incidents and disaster operations.

When I was interviewing Senator Petris he said something very interesting about his conduct of the investigation into the fire. He said that one of the lessons he had learned was that if you really wanted to know what's going on, ask the people on the bottom of the pile. He said that bosses have turf to protect, and that you get the most honest responses from the action people who are out doing the job in the field.

He felt that the closer you got to the action, the more people were inclined to be uncompromising, upfront, and forthright about what happened – what went well, what went bad, and how to fix it.

That's what I want you to do. Go on your own fact-finding tour. These issues are too important to the lives of the people you are responsible for. Get out of your office, go find a worker type out in the field, take them aside to some place they can relax (go buy them a cup of coffee or lunch), and ask them a couple of key questions.

Tell them you will respect their confidentiality and ask them to respect your fact finding process by not discussing the interview. This will give them an out if their boss asks them what was discussed. They can say that they were told to refer all questions to you, and not to talk about the interview. All good bosses should have no trouble with you talking to their troops.

If you are a business manager or building manager, you need to understand that you are the critical third part to a critical incident response. The actions of you or your staff must mesh with those of police and fire. You have a vested interest in this process and should talk to your elected officials about conducting a fact-finding and make sure that the results are shared.

Most agencies may have trained specific personnel, but the numbers of these special people are very small and there is no guarantee that any of them will be available if an actual terrorist event occurs. The big gap from my perspective has been that none of the line level patrol officers and firefighters has received any of the training and drillings that they need to respond to a terrorist incident.

This extends to the problem that none of the line police officers or firefighters have participated in actual drills together. The only way that we really learn how to function properly as a team in a critical incident is by training and drilling together. We're so short handed that management is reluctant to take these officers off the street and spend the significant time it would take to train all of them how to work together. Because of this problem, a few elite people such as a SWAT team or Hazmat team may have been trained, but none of this training has trickled down to the line police officers and firefighters who are going to be the actual first responders to a terrorist incident.

This training and drilling process is especially important when you consider the role that building managers and managers of facilities such as sports arenas, high rise buildings, and shopping malls play in the emergency response process. They have been completely left out of the emergency training and drilling process. They're the critical third part to any emergency response process because of their unique knowledge of their facility. For the most part they have received no training on how to assist police and fire in trying to handle a large-scale critical incident in their facility.

So, go on out and grab some of the real first responders – the field police officers and their Sergeants, the fire fighters or fire Captains, and ask them the following questions:

- Do you have immediate access to your Department's Terrorism Response Plan, and can I see it?
- Has everyone in your team trained on this plan?
- Specifically, what terrorism training have you had, if any?
- Have you received any new equipment specifically designed to help you during a terrorist incident, such as a new gas mask filter?
- Police: Do you have immediate access to a rifle in your car to combat a person with an automatic weapon?
- Fire: As a First Responder Operational person, do you have immediate access to proper Personal Protective clothing for Chemical or Biological incidents?
- When was the last terrorism drill in which you participated?
- Was this drill(s) with other emergency responders?
- What are the top 10 terrorist targets in your city or county?
- Were these targets made known to you by your management?
- Do you have a response plan for any or all of these targets?
- If you do have a response plan, is it readily accessible and can I see it?
- Have you inspected or walked around any potential targets within your area of responsibility, such as your patrol beat or fire district? This would include high-rise buildings, sports complexes, schools, and shopping centers.
- If such an inspection was done, are the results written down and available to all first responders?
- Have you discussed the principles of how you would respond to a terrorist act with any of your supervisors such as a police Sergeant or fire Captain?
- Have you had any training on the Incident Command System?
- Can you explain the concept of Unified Command?
- Does your agency have a specific person who coordinates all information and training regarding terrorism?
- Who is this person?
- Have they been teaching classes and are they accessible to you?
- Do you think the management of your agency has placed a sincere emphasis on training for critical incidents and terrorist acts?

Please remember that I am approaching this from a very narrow perspective – which is the response by local emergency services to a critical incident such as a terrorist

act. I think that by starting some honest dialogue regarding our shortcomings and trying to fix them if we find them, we can all benefit by having the first responders prepared when one of these incidents occurs in our jurisdiction.

Unified Command at a Terrorist Incident

The Incident Command System (ICS) has been almost universally adopted as the method of rapidly organizing a critical incident, such as a terrorist attack. The eight jobs in the Incident Command System will allow us to rapidly organize a confusing set of circumstances. If all the agencies involved in the incident are using the same eight critical jobs to manage their agency, the cooperative effort of all the agencies will increase dramatically. The principal is that of having all responders "singing off the same sheet of music," so that we don't waste valuable time learning each other's organizational framework.

California has mandated the use of ICS at any critical incident or natural disaster for which reimbursement will be sought from the state. This law that went into effect in 1996 was a direct outgrowth of the disastrous Oakland / Berkeley Hills fire of 1993. Valuable time was wasted during the attack on the fire because all of the mutual aid agencies that responded used a different method of command organization. This led to significant confusion between the responding agencies. Subsequent investigation and reform by the state legislature resulted in the passage of California's Standardized Emergency Management System -- or SEMS -- law. It is this law that outlines the principles of ICS and the eight critical jobs it encompasses. With regard to the job of Incident Commander, it is important in the context of "who's in charge" to talk about the ICS concept of Unified Command.

Unified Command speaks to the issue that all of the major players in an incident need to get together to share information, resources, and responsibility for the smooth delivery of effective service. But, as in all events, there can only be one boss, one "shot caller," directing the focus of the group, and setting the group's goals.

The image of a triangle helps to convey this concept. In an organizational chart there is usually a box at the top for the Incident Commander. I want you to think of the Incident Commander position in this chart as a triangle in which multiple agencies' bosses can reside. In our terrorist incident, there are three major players: local fire, local law enforcement, and the FBI. There could certainly be others, such as public works for heavy equipment and major infrastructure damage, but let's stay with the main three for now.

This whole system of "who's in command" and Unified Command only works if all agencies are aware of each other's primary needs. The Fire Department must have crowds kept back and clear streets to move in heavy equipment. Law enforcement needs to have evidence preserved and witnesses identified. The FBI needs to have extensive cooperation and support for many days and even weeks from both the local fire and law enforcement to preserve the scene and collect evidence.

The task of Incident Command during a terrorist incident is a co-operative effort between these three main players - the local Fire Department, local Law Enforcement, and the Federal Bureau of Investigation.

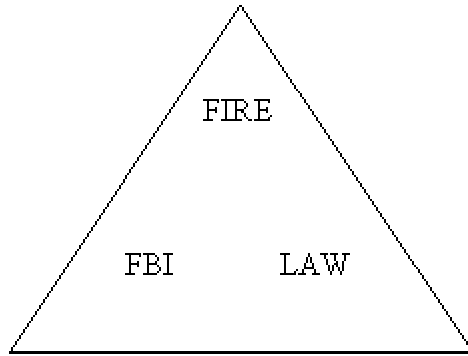
In the past there have been incidents where these three groups did not work cooperatively. This is not the case today. Old style inter-agency rivalry has given way to an era of better sharing of responsibility and cooperation. Today, faced with shrinking budgets and manpower, a growing terrorist threat, and a media that can be highly critical of emergency response agencies, this most destructive behavior has all but been eliminated.

The progression of incident command responsibility at a terrorist act will pass through these three significant groups, following in time order of what is needed most as the incident unfolds. In order, the Incident Command will rest with:

- LOCAL FIRE DEPARTMENT. To assume command during the initial fire, rescue, and medical response to the incident.
- LOCAL LAW ENFORCEMENT. To assume command after the fire-rescue-medical threat has been neutralized and to conduct preliminary investigation until the FBI is prepared to assume command. During the time that the Fire Department is in command, the local law enforcement will follow the Mass Casualty Incident (MCI) Protocol for Law Enforcement while it is preparing to assume command, along with getting itself organized.
- THE FBI. Under the Federal authority of Presidential Decision Directive 39, the FBI is the lead investigative agency in any act of foreign or domestic terrorism, and will assume command of the incident and subsequent criminal investigation. It will take some time for the FBI to have sufficient resources on the scene to assume command. It is critical that local law enforcement remains on scene to assist and support the FBI in this mission after the role of Incident Command has passed to the FBI.

As the three main players come together on the scene, they will form a unified command group. The first priority will be to handle all of the fire, rescue, and medical problems. The Fire Department will move to the top of the triangle and set the goals for the operation. Once the fire, rescue and medical efforts have ceased, the local law enforcement agency will move to the top of the triangle and assume incident command.

(continued on next page)



UNIFIED COMMAND
With FIRE as Incident Commander

This does not mean that law enforcement sits around waiting until fire has relinquished command. Local law enforcement will be responsible for following the principles of assisting with an MCI during the time that the Fire Department is in charge.

When Incident Command passes to law enforcement, the law officer in charge will then set the goals for the operation, and begin full conduct of the preliminary criminal investigation. This will include identifying and taking initial statements from potential witnesses and victims, along with crime scene preservation and any emergency follow-up actions or evidence collection.

When the Fire Department begins to wind down its functions of fire-rescue-medical response, the fire and law commanders will agree when incident command will pass to law enforcement. When this occurs, simultaneous broadcasts should be made on both the fire and law enforcement channels so that all personnel understand that incident command has passed from the fire service to law enforcement.

Also at this time, the specific location for the law enforcement command post should be repeated via radio so that there is no mistake as to where the command post is located.

It is essential that a Fire Department command level officer remain in the command post. This will ensure continuity of information, and also provide an officer who can direct fire resources if they are needed during this time.

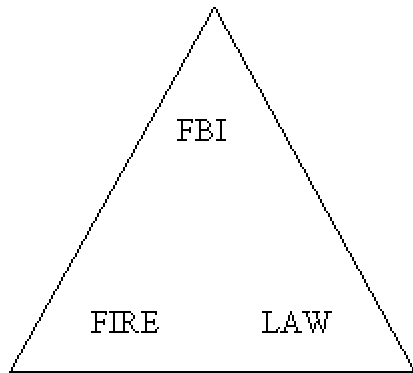
Remember, until someone makes the call that the incident fits our definition and is an act of domestic or foreign terrorism, the event is basically the local jurisdiction's homicide, assault, vandalism, bombing, etc.

The FBI will usually dispatch an initial Special Agent as soon as the incident occurs, as a direct result of just being in your town and monitoring radio frequencies. **If you even slightly suspect that you are dealing with a possible terrorist event that fits our definition, call the FBI out immediately.** Depending on your location, it may take a

few minutes to a few hours to get a Special Agent at the scene, and the lost time for coordination can be harmful to later efforts.

It is always better to have the FBI on scene as soon as possible. In the event the incident is a terrorist act, the Bureau will be up to speed and be able to assume command responsibility without any loss of information. If the incident develops, and it is a local crime such as a homicide or bombing, the FBI's presence will give you another well-trained investigator on scene as a valuable resource for both investigative ideas and evidence-collection issues.

The FBI also provides both technical support and special resources you may not have at your local level. However, it can be several hours before the FBI has assembled a full command team and they are ready to take over the incident. During the interim, the local law enforcement agency will assume the position of Incident Commander, while coordinating in the Unified Command with the Fire Department and the FBI staff on scene.



UNIFIED COMMAND
With FBI as Incident Commander

When the FBI team has been assembled and is in place, the Bureau then will assume command of the incident. The FBI might be able to respond its evidence collection teams to the area fairly quickly to assess the evidentiary problems and get a handle on how much staff they will need and what specialized equipment they should bring. The FBI has its own policies on evidence collection, so if you believe this is a terrorist event, it is better to seal the area and let Bureau evidence technicians collect the evidence rather than filling up your property warehouse and creating a major chain of custody issue. If some evidence needs to be preserved on an emergency basis, this should be done for later transfer to FBI custody. Since almost all of our response to an act of terrorism will be after the fact, evidence collection issues will be crucial for the arrest and conviction of the suspect(s).

The important thing to understand at the local level is that once the FBI agents have assumed command, they will still need continued support and assistance from the local law

enforcement and fire agencies. They will need help with traffic control, body and evidence recovery, scene security, and a host of other critical tasks.

The FBI, in order to better coordinate the federal response to an act of terrorism, will establish its own version of the Emergency Operations Center called a Joint Operations Center or JOC. This is the location where all federal agencies will first report and work out of for the duration of the incident, and it corresponds to local government's EOC.

In recent discussions with Special Agents of the FBI, they indicated that they will try to co-locate the JOC at a local jurisdiction's EOC if possible. At a minimum, they will try to provide a command level officer to stay in the local agency EOC to facilitate direct communication between the groups involved in the unified command, and to facilitate the sharing of resources, personnel, and information.

In order to better function together it would be helpful to work out of one central EOC. The FBI's establishment of a separate JOC is based on the large numbers of agencies and support staff that could be called in to help at a major terrorist event. This is a legitimate concern. In the event the incident is a large one, the Incident Commander should be looking for an area large enough to accommodate these priorities so that both facilities can be at the same location.

As the local agencies' involvement winds down, fewer staff will be necessary, until finally the JOC will become the only coordination point for the incident. When on-scene activity ceases, all follow-up investigative activity will be the responsibility of the FBI.

As you can see during each of these phases, a different group will be moving to the top of the triangle. But all will still be together working on the issues, and sharing concerns and information in the Unified Command concept.

About the Author

Lt. John Kane is Watch Commander in the Patrol Division for the Sacramento, Calif. Police Department, and is also in charge of the department's Disaster Planning and Emergency Preparedness. He is an adjunct instructor at the Emergency Management Institute, teaching law enforcement response to disaster events and terrorist incidents. As a member of the California Governor's Committee of Law Enforcement Specialists in the Standardized Emergency Management System, he helped write and develop the "California Law Enforcement Guide for Emergency Operations" manual.

* * * * *

Public Works and Terrorism

By Richard Evans

Not many years ago public works people were seldom, if ever, concerned about terrorism. However, events such as the destruction of the World Trade Center Towers, the bombing of the Federal Building in Oklahoma City, the assassination of the Mayor and a Supervisor in San Francisco, anthrax scares in a number of cities, and other incidents have pointed out the need for public works and building management people to become involved in building and system security matters.

Building security is a mixed bag at best, especially for public buildings which, by their very nature, must be open to the public on an almost unlimited basis. This is even more true when the buildings are populated by elected officials. The issue of how to provide access and yet maintain a level of security is complicated at best.

To begin with, you cannot accomplish these goals by yourself, nor can you do it by using local law enforcement people. Not that they are not competent, far from it, but they are often too close to the matter to be totally objective. Nor can you just go out and buy magnetometers, x-ray machines, and hire a couple of security guards and think that the job is finished. Although this might be what you end up doing, you should first make a serious effort to analyze the problem, review the alternatives, seek the advice of trained professionals and then refer to the body politic the range of solutions and your recommendation for the preferred alternative.

You might want to visit your local airport, jail, or courthouse to see the levels of complexity in equipment, operations, and management of security systems. During these visits you need to discuss with the people in charge of the facility issues relative to maintenance, operations, and management of their systems. You might even enlist these people to serve on an advisory board for you during the decision making process. This will, of course, depend on the level of confidentiality you need to maintain.

There is a wide range of cost and quality for the various pieces of equipment that are available. However, it can only function to the level of the people that are hired to operate it. Again, there is a wide range in the cost and quality of the people that you might hire. With all of this in mind, it is now time to begin the quest for a security system for your building(s), including the people to manage and operate it.

There are several sources that might offer a high level of expertise for your project. These include utility company security employees (retired or on loan), retired FBI or Secret Service employees, retired law enforcement officers, and retired military personnel to name a few. If you are in a time crunch, you may be able to get some pro-bono help from any of the above to help you get started. Remember, check their qualifications before accepting any help -- free or not.

The first thing that you should do is try to find an expert in the field. You might circulate a “Request For Proposal” (RFP) that asks for interested parties to apply and bring with them a list of their accomplishments, experience, background, training, and whatever else that might support their qualifications for the project. At some point in time you should have the candidates develop a cost figure for their services, but you may want this to be delayed until you have developed a “short-list” of bidders for considerations.

An RFP allows you to select the party that is most qualified, rather than the one with the lowest bid. After all, you are not building a sewer, you are developing a security system. Whatever the process, the experts need to include with their proposal, recommendations regarding management and operation of the system. Also, you might want to limit your list of consultants to firms that do not have any connections with manufacturers of security equipment.

Further, you do need to include in your RFP their recommendations for operation, repair, and maintenance of the system(s). This should also include training for the operators when you present your recommendations to the decision makers. They will be the best people to answer technical questions regarding the equipment, etc. They should also be of value when you are developing recommendations for how the system is to be operated and by whom.

Depending on who the occupants are of the building that you are trying to protect, you may want to make them aware of the process. You may also want to make your local law enforcement people aware of what you are doing, especially if they are going to be charged with the ultimate responsibility for supervision of operation of the system.

Now we come to a significantly different part of the process: selecting the people to operate it. There are a number of alternatives. These include hiring a private security firm, using local law enforcement officers (police or sheriff personnel), retired law enforcement or retired military people, or using building and grounds patrol people. Once again, discussions with others, such as those you visited, will give you a lot of help in selecting alternatives. Once again, cost will be a significant part of the equation in your decision making process.

No matter whom is selected, they need to be fully trained, not only in the operation of the equipment, but in the way they conduct themselves, deal with problem people, diversions, questions, etc. These are often the first contacts visitors have with your organization. This means the security people need to make sure that this is a good contact, one that is not confrontational, but one that tries to maintain a secure building.

We need to stress the point that the vendor of the equipment you purchase should be involved in the training. Further, your consultant may be able to advise you relative to training the security people regarding their duties and how best they are performed. The performance of your security people needs to be monitored on a regular basis.

Internal Security

By now most people are familiar with the security provided at airports and the way it is managed, so that security for public buildings need not be a threat.

However, tenants and visitors alike must not be lulled into a false sense of security. Just because there is a guard at the gate does not mean that the place is totally secure. Therefore, you may want to maintain an internal security system that will provide additional protection.

There are a number of ways to provide internal security. These include keyed or keyless entry systems, closed circuit television systems, roving patrol people or any combination of the above. All of them have cost impacts, and depending on conditions, have liabilities. Building configuration may make closed circuit television difficult if not impossible. Keyed or keyless entry may be very expensive. And roving patrols likewise have their limitations.

In fact, you may need to develop different levels of security for various areas inside the building. This may require some special effort and perhaps some relocation of some officials, but this should not be very difficult to do. Having occupants of the building involved in the planning process should facilitate any relocation issues.

The issue of intruding on people may also affect your decisions. This is an area where your agency's legal staff may be able to advise you. Actually, your agency's legal staff should be involved in the entire process, from consultant selection, through the RFP and the conclusion of the project. Again, on your visits to other facilities, discuss internal security with your hosts.

Assessing Facilities, Infrastructure Security

So far, we have dealt with building security.

However, public works and general services people need to be aware of security needs for other facilities and systems under their jurisdiction. Sewage and water collection, distribution and treatment facilities, sports complexes, arenas, theaters, museums, transit stations, schools and hospitals are all potential targets.

Condition assessment analysis is a good tool for determining the condition of these facilities and systems that are needed to serve the people. These analyses look at structural conditions, life-safety and code compliance, maintenance history, usability, and a number of other items that need to be reviewed on a regular basis to ensure that the money spent on the operation and maintenance of the infrastructure is done so wisely.

Likewise, a vulnerability assessment could and should be included in the analysis. This would use some of the same people listed above and help clarify decisions that need to be made, especially with regard to use, repair with upgrades, and/or replacement. But

now that you are considering vulnerability you need to bring in experts who are qualified to assist you in this part of the process.

We have moved past the use of chain-link fences, barbed wire or razor wire. Granted that these things will keep out many, but those who are determined can easily get past such low-tech devices. And you can not use these devices to protect public buildings, although they are somewhat effective for protecting operational facilities (treatment plants, transit stations, etc.), especially when used in concert with closed circuit television, high intensity lighting and fences equipped with motion sensors.

A vulnerability analysis will assist you in ultimately selecting the optimum way that you might protect you facilities.

A vulnerability analysis looks at what might be done to damage the operation of a facility or system; what is located nearby which, if damaged, might have an impact on the quality of life, health, or economy in adjacent parts of the area; and what alternative systems might exist to replace those that are damaged or destroyed. Is it practical to protect these facilities or should or could they be relocated to reduce or eliminate the risk? Finally, how would your jurisdiction recover if the subject of your study was damaged or lost to use?

A number of factors will complicate your work. These include the age of your infrastructure, who has jurisdiction (public or private), existence of redundancy, the practicality of replacement or redesign, and the availability of funding to complete the necessary work. A half completed project is probably worse than no project at all.

You cannot keep people out of a subway system nor can you build a wall around a watershed. Transportation facilities, railroads, airports, and highways allow the movement of thousands of people and millions of pounds of goods daily. It is impossible to keep out those that are intent on doing damage, yet we must do all that we can to make conditions as safe as possible.

Look at the risks and try to develop answers to the following:

- If we cannot eliminate the risk, can we develop a warning system that will activate a response that will minimize it?
- Have we established and tested evacuation routes?
- What can be done to mitigate the risk? Relocation?
- Is there, or can you develop, a recovery plan?

Regardless of the complexity of your buildings and facilities, some very basic steps need to be followed.

These include key control, attention to keeping windows closed and locked at night, alert security staff, evacuation plans that are tested on a regular basis, and a building population that participates in the same way a “Neighborhood Watch” group does. And, no

one is allowed to by-pass the security devices – no one, no favorites, just provide the same level of scrutiny for all. No exceptions shall be allowed. Once again, you should not try to convince the tenants that they are perfectly safe, because they are not. A false sense of security is the most dangerous environment that you can provide.

About the Author

Richard Evans is a registered professional engineer in civil and traffic engineering, and is the former Director of Public Works Department for the City of San Francisco. He was the Director during the October 1989 earthquake. He is an adjunct instructor for FEMA's "Consequences of Terrorism" course.

* * * * *

Chemical and Biological Terrorism

By Vaughn E. Wagner, Ph.D., B.C.E., M.E.

Assistant Professor

Environmental Health Science

Salisbury University

Terrorists by definition seek to create fear and panic. Their motivations are legion and one rarely recognizes, until an incident happens, that the terrorist is in our community. Driven by ideology, grievance, anger and other sociological issues, they attempt to make their presence felt by sudden and dramatic means. Injury, disruption, and death are their goals. Other objectives include media attention, publicity for their cause, and retribution for real or imagined grievances. Terrorist activity is a type of guerrilla warfare. A terrorist may be part of a highly organized, well-funded unit or may be a single, disgruntled employee. Potential for terrorism exists in every community. Public awareness, education, and training will help foil some incidents and mitigate others.

Understanding the nature of chemical and biological terrorist incidents can be challenging to those charged with the responsibility for response and mitigation. It is the goal of this paper to shed some light on this controversial and misunderstood facet of emergency response. In order to understand the potential threats, consequences, and vulnerabilities resulting from the intentional releases of chemical and/or biological agents, a basic review is needed of environmental and agent components affecting toxicity/infectivity. Also, the terms toxicant and toxin as used in this paper mean two different things.

The first relates primarily to those synthetic chemicals produced by man (insecticides, solvents) while toxin refers to chemical metabolites produced by living organisms (T-2 mycotoxin, botulinum toxin). An understanding of toxicological and microbiological principles, choice of chemical weapon or biological weapon agent, ease of acquisition, efficient aerosolization and dissemination, are key ingredients of the terrorist equation for effecting mass casualties and emotional trauma.

Bioagents most likely to be used in terrorist attacks are anthrax, botulinum toxin, and ricin. Chemical agents may include cyanide blood agents; mustard gas-type vesicants; and organophosphate nerve agents. Less toxic substances could be used, however, to cause large-scale injuries to the community. Examples are off-the-shelf insecticides such as malathion or diazinon (cousins of the nerve agents). Carbamates such as carbaryl are also good candidates.

One of the principal advantages of chemical and bioterrorism agents is their extreme toxicity in small quantities. These agents must have the ability to form and be delivered in respirable aerosol concentrations (10 μm or less) to result in mass casualties. The settling rate of aerosol droplets of this size proceeds very slowly and will drift for

enormous distances at low wind speeds. Consequently, the ability of chemical and biological agents to generate aerosol droplet clouds is a necessity in order to be effective.

Of major concern is the accessibility of specific related compounds such as the organophosphate (OP) insecticides and the use of peacetime delivery systems such as insect sprayers, dusters and ULV foggers to disseminate the agent. Target delivery systems would be heating/ventilation/air conditioning (HVAC) systems and/or water reservoirs in high use areas (governmental buildings, shopping malls, or community centers).

CHEMICAL AGENTS – Blood and Choking Agents

Chemical mass casualty threats are most likely cyanide products (blood agents) and chlorine/phosgene (choking agents). They are industrial chemicals with widespread application and widespread availability. A terrorist may choose to redirect legitimate chemical sources to criminal terrorist purposes.

Cyanides act rapidly, causing death in minutes. Intravenous therapy may prove effective, but it is unlikely to be available in time unless there is advanced warning and preparation for the attack. Treatment requires fixation of the cyanide ion. Drugs such as intravenous thiosulphate and DMAP (4-dimethylaminophenyl-hydrochloride) are needed to achieve this cure.

Pulmonary agents such as phosgene may not cause serious initial discomfort. However, over time (within hours), they produce pulmonary edema and acute respiratory distress. Phosgene releases hydrochloric acid as it breaks down in the body. Its major medical impact, however, comes from its acylation reactions in the lung at the alveolar/capillary membrane. This leads to leakage into the interstitial portion of the lung.

Phosgene is treated with supportive respiratory therapy, to battle hypoxemia (unoxygenated blood from fluid in the lungs) and hypovolemia (due to the internal blood loss). Although pulmonary agents are not considered priority battlefield threats, their large-scale use by terrorists would most likely saturate available respirators.

BLISTER AGENTS (VESICANTS)

Mustard gas was one of the first chemical warfare agents, and remains a staple in many arsenals today. Only a minority of victims dies from the initial exposure. However, they require a long period of treatment before recovery. Sulfur mustard agent does not irritate the skin, but rapidly penetrates it. Within hours, it can cause blistering, alkylation of DNA, and bone marrow suppression. Mustard dissolves rapidly to form extremely reactive ions that bind to intra- and extra-cellular enzymes and proteins. This leads to cellular death and inflammatory reaction, including protease digestion of anchoring filaments in the skin and the formation of blisters. Vesicant exposure requires extensive supportive therapy as provided by any hospital intensive care unit.

NERVE AGENTS

Acetylcholine is a biochemical neurotransmitter that links nerve cells to muscle and organ cells inside the body. When nerve cells are stimulated, they release acetylcholine into the space (synapse) between the different types of cells, stimulating muscle cells. An enzyme called acetylcholinesterase rapidly breaks down (hydrolyzes) the active acetylcholine, permitting its "reuptake" to the nerve cell. Chemical agents known as nerve gases prevent the acetylcholinesterase in the synapses from neutralizing the active neurotransmitter, assuring that the muscles or organs continue to be stimulated, leading to convulsions and death.

Nerve gas was invented in the 1930s in Germany and is based on organophosphates. Various insecticides, such as malathion, can be considered a weak form of nerve agent. Sarin is one of the most widely feared nerve agents because it is relatively simple to synthesize, as well as having high lethality. VX, while considerably more powerful, is commensurately much more difficult to produce. Its use would tend to indicate a state-sponsored attack.

Therapy for nerve agents is atropine and an oxime such as 2-PAM Chloride (2-pyridine aldoxime methyl chloride; also called pralidoxime chloride). Even after surviving challenge, patients may enter an epileptic state in which they require anxiolytics such as diazepam (valium). Oximes attach to the nerve agent inhibiting the cholinesterase and break the bond with the agent, enabling the enzyme to resume normal activity. Once atropine and oximes are administered, supportive respiratory therapy may be needed.

Valium may also be administered as an anti-convulsant. Pyridostigmine Bromide (PB) is also an interesting pre-medication. It acts as a relatively mild, reversible nerve agent. PB is a carbamate that temporarily binds to the molecular sites and denies the nerve agent a binding site. Later, PB comes unbound, and the cell resumes normal activity.

BIOLOGICAL TERRORISM

Leading biological agents are anthrax, tularemia, plague, viral hemorrhagic fevers and smallpox. Toxins are usually classed as biological agents, although they are chemical by-products of biological organisms. Toxins are powerful poisons, but they do not reproduce in the host's body, as bacteria and viruses do.

The major categories of biological agents are bacteria, viruses, and toxins. From a medical perspective, one may be vaccinated against either a bacterial or viral illness and build up immunity over weeks or months. However, bacteria are small living organisms that may be treated by antibiotics. Viruses, on the other hand, will run their course and are not susceptible to antibiotics. Viruses are also contagious from person to person, while many bacteria are infectious but not contagious. One has to be directly exposed to get the disease. Although there is much less that medical science can do to treat viruses, they are also much harder for potential terrorists to produce. For instance, viruses need to be grown

in eggs, animals, or a bioreactor, since they cannot survive and reproduce independent of a host. Bacteria, on the other hand, may be simply fermented in a growth medium and produced in quantity.

Terrorist-initiated scenarios that could intentionally expose citizens to biological agents are:

Bioaerosol development and dissemination via man-made delivery systems

Specific bio-agents such as bacterial and fungal agents are ubiquitous in the environment and routinely develop in man-made delivery systems. These systems include HVAC systems as well as water displays and reservoirs. Terrorist development and dissemination of bioaerosols containing anthrax, botulinum toxin, or fungal mycotoxins are feasible. High-use community areas such as domed stadiums, shopping malls, subways, and governmental complexes would be prime targets.

Hazmat incidents involving biomedical materials

This category would include the intentional discard of medical wastes and infectious tissue material into or onto a target site. These substances would be of a human and/or animal tissue/blood sample type utilized in drug/medical research. The health effect of these types of terrorist-initiated releases would be limited. The basic impact would be more of an emotional nature.

Shipment of Class III pathogens

Packaging containing Class III pathogens (anthrax, *C. botulinum*, and plague are examples) are routinely shipped throughout the country from type collection laboratories to medical and microbiological research facilities. It is estimated that 10 percent of the approximately 80,000 shipments of microorganisms throughout the United States are Class III pathogens.

Shipment is by common carrier. Shipments involving 50 ml (or less) may be by passenger aircraft or ground transportation. Shipments that are 4 liters (or greater) must be by cargo aircraft.

The concern for emergency responders is that a terrorist group, disgruntled graduate student, or angry medical researcher might target a shipment; intercept the package containing the bioagents; and use the contents as seed stock for biological weapons production. Even if this is not the case, the placement of the stolen container at a high-use area would result in citizen trauma and panic. Intensive media coverage would also be a goal of the terrorist group.

Use of biological agents for agricultural pest or public health pest control

Bacillus thuringiensis (BT) strains have wide use as an agricultural and public health (mosquitoes, black flies) insecticide. The BT organism and its delta-endotoxin toxin adversely affect the targeted insect and effectively control the pest. BT is not a human pathogen. However, BT is closely related to the anthrax organism, *B. anthracis*. BT is also a spore-former whose parasporal bodies are cuboid or diamond shaped as opposed to anthrax's cylindrical or oval spores. BT is mass-produced in the U.S. by a fermentation process. The resultant crystalline spores and delta-endotoxin are formulated as liquid concentrates, powders, or granules.

The concern from a terrorist standpoint is that spray and granular equipment designed for BT dispersion could be easily adapted to a bioaerosol dispersion of anthrax spores. Also BT formulations could be contaminated by anthrax and applied by air or ground spray equipment used in mosquito control and agricultural pest activities. This is particularly relevant to populated areas, as mosquito control is usually conducted in highly urbanized or recreational areas.

BIOLOGICAL AGENTS - BACTERIA

Anthrax is often considered the leading biological threat agent because of its unique combination of high lethality, relative accessibility, and relative ease of covert employment. Its inhalation form has a mortality rate once the infection sets in and symptoms are present. However, there is a vaccine to make one immune to anthrax. In addition, exposed individuals can start treatment with antibiotics to prevent onset of symptoms. This may be done while also getting vaccinated, so that natural immunity is achieved before discontinuing the antibiotic regimen (about eight weeks).

Anthrax is endemic worldwide and forms a robust spore. Animal outbreaks are usually associated with dry weather, when dust containing old spores is then inhaled or ingested by animals. About 8-10,000 spores are considered the minimal infective dose. Anthrax can manifest itself in cutaneous or gastrointestinal forms, if the microbe infects cuts on the skin or is ingested. However, inhalational anthrax is considered the most deadly.

Spores in the 1-10 micron particle size are inhaled deep into the lung alveoli. There the spores may germinate and become vegetative. They are identified by the immune system and transported to lymph nodes in the mediastinum; the area around the heart and lungs. Anthrax spores are then ingested by white blood cells known as macrophages (macro = large, phage = eat). However, instead of dying, the anthrax has a capsule that protects it and permits it to reproduce inside the macrophage. It effectively releases toxins from host cells, leading to edema and septic shock (meningitis in about half the victims). Once the infection takes hold, even antibiotics are not effective, since the major impact is from the released toxins. The incubation period of the disease is considered to be 1-6 days by USAMRIID experts.

Even at late onset, the course of the disease is similar. The first symptoms are nonspecific and flu-like. There may be an "anthrax eclipse" during which the patient feels better. However, within a day or so, breathing becomes extremely difficult (dyspnea) and the patient dies shortly thereafter (similar to septic shock). It is the start of this second stage when most patients would seek hospitalization.

Since there are virtually no cases of respiratory anthrax, emergency room doctors may not recognize it immediately. With dyspnea, a sputum culture and an x-ray will be ordered. The sputum culture will come back negative, since the disease has taken hold in the lymph system rather than the lungs. The negative finding will probably trigger significant curiosity, since influenza or pneumonia would come back positive. An x-ray will reveal an enlarged mediastinum due to the anthrax edema.

It is at this point that critical care specialists may suspect anthrax, and move to preventively treat patients with similar symptoms while awaiting results of dispositive tests. Such tests have to be done in special facilities and may take 24 hours. Other evidence for a differential diagnosis may be drawn from autopsies. About half of the victims will have meningitis (a destructive inflammation of the brain).

All persons in the impacted area may need antibiotic prophylaxis. The antibiotic of choice is ciproflaxacin, until sensitivity tests determine if the microbe is sensitive to the tetracycline family or ampicillin (oral penicillin). In general, antibiotics have a limited shelf life (about 3 years) and are purchased at the rate at which they are expected to be used. There are few stockpiles of large amounts of antibiotics, especially ciprofloxacin or other fluoroquinolones. The US Centers for Disease Control is working on the stockpile problem.

Another treatment approach is through bacteriophages ("eaters" of bacteria). They are viruses that attack bacteria. Bacteriophages attach to the cell, inject their DNA and reproduce. When the cell bursts, up to 200 new bacteriophages are released, which pursue the same type of host cell and repeat the process. There are bacteriophages that are specific to anthrax. Some bacteriophages have been tried against sepsis and have survived and reproduced in a living host. It may be possible to develop bacteriophages that are able to attack anthrax even when they are engulfed in the macrophages.

BUBONIC PLAGUE

Bubonic Plague is the disease that devastated Europe in the 14th century, killing perhaps one-third of the population. Plague is still endemic around the world, including the southwest U.S. However, it is susceptible to antibiotics. Bubonic plague is spread by fleas on rats that then infest humans. However, after the disease spreads from the buboes (certain lymph nodes) to the lungs, it becomes pneumonic plague. The pneumonic form can be spread by droplets from human to human (coughing) and is highly contagious.

VIRUSES

Smallpox is one of the most prolific killers in history. Over 100 million died in this century alone before smallpox was declared eradicated (around 1972) by the World Health Organization. Currently, the only legally declared stocks are held by the U.S. and Russia. The destruction of the last samples has been postponed at the request of the US, so that work may be done to find a medical treatment for the disease. This may be important if additional stocks have been withheld and remain viable.

The U.S. stopped vaccinating against smallpox shortly after its formal eradication was declared. We retain about 16 million doses of vaccine (basically vaccinia or cowpox pustules scraped from intentionally infected calves). However, these stocks are failing quality control checks as they age, and moisture appears to be penetrating the package seals. Nevertheless, authorities believe the vaccine is still effective. They have not used it lately, however, since an antidote supply has also become questionable. The US Food and Drug Administration (FDA) insists that vaccinia immunoglobulin (VIG) be available to anyone who takes the vaccine, especially since the vaccine strain is very reactinogenic.

A new smallpox vaccine and VIG are being created for the military. Smallpox vaccine is very important, in that it can prevent the onset of symptoms even if one has recently been exposed. Victims are considered to be contagious from the time their symptoms start to appear until their pustules scab over.

TOXINS

Toxins are poisons that biological agents produce. Small quantities can cause fatalities. However, most toxins will not penetrate the skin (exception: the fungal mycotoxin, *yellow rain*). Toxins do not reproduce themselves in the host, as biological agents do. Botulinum is one of the most potent toxins on earth. Interestingly, it tends to work in an opposite way to a nerve gas. It prevents the uptake of the neurotransmitter acetylcholine. Thus patients have a characteristic lethargy and drooping eyelids. Death occurs when the diaphragm no longer contracts, and breathing stops. Availability of artificial respirators is key to overcoming a botulinum attack. The effect wears off if breathing can be maintained.

Ricin is another potent toxin, which can be derived from the common castor bean. Ricin does permanent damage, even if the victim does not die. This plant toxin appears to have been used in the past as a bioagent weapon.

NATIONAL ACTION NEEDED

The effective dispersion of chemical and biological agents can be accomplished in a variety of ways. Chemical or bioaerosol dissemination over widespread areas is feasible through aircraft-mounted aerosol generators used in insect control. In a confined space area

such as a HVAC system or a discrete water supply, a more limited assault involving hand-held motorized spray application equipment would be highly successful. Direct contamination of food products and food preparation areas would be the easiest target for the terrorists.

Considering all the factors and the uneasy political times we live in, there is a very good possibility of terrorist attacks utilizing chemical and biological agents in the future. Most of the emergency response community agrees that this threat has to be taken seriously. Obviously, monitoring and responder training is most effective prior to an incident.

Serious consideration should be given to the development of "real-time" biological sensors; establishment of tighter regulations dealing with the acquisition and use of CB agents, as well as the equipment used for aerosol dissemination. Also, high on the priority list are increased public awareness and education as to the threat posed by BC agent assaults, coordination between all intelligence, training, and military communities and increased training of local emergency managers.

On a more practical note, vaccine, antibody and antidote research and development need to be adequately funded. The responder community also needs the development of adequate and "user friendly" protective equipment. Creation and maintenance of regional biological/chemical task forces would go a long way in assisting the local responders in mitigating "agents of mass destruction" incidents.

LOCAL HEALTH DEPARTMENTS: INITIATIVES FOR TERRORIST-SPONSORED ATTACKS

The role of the local health department is to provide leadership to the public health and medical communities in a coordinated effort to detect, diagnose, respond to, and prevent illness that could result because of chemical or bioterrorism. These tasks are an integral part of local health departments' overall mission to monitor and protect public health.

In this regard, a strong and flexible public health infrastructure is the best defense against any terrorist-initiated attack. Local initiatives should include the strengthening of disease surveillance and response at the local level to detect and contain injuries/diseases caused by chemical or bioagents. Rapid response with accurate information provided to the media helps to forestall panic.

A terrorist attack utilizing chemical and bioagents initially may be invisible and undetected. Chemical releases would be easier to detect, as the onset of symptoms would be relatively immediate. The release of a biological agent or chemical toxin might not have an immediately visible impact because of the delay between exposure and onset of illness. Initial responders to such attacks would include local health officers, hospital staff,

members of the outpatient medical community, and a wide range of response personnel in the public health system.

Thus, the local health department has a major responsibility to improve the public health community's preparedness to detect injuries or illness that are a result of a chemical or bioterrorism threat. Local health department initiatives therefore should include the development of the appropriate public health structure and contingency plans to respond effectively in the event of a terrorism-initiated incident. An integrated approach with public safety, police, and emergency responders is extremely valuable if instituted PRIOR to an event. This allows for efficient utilization of specific strengths toward effective management of the event.

Local Health Department Initiatives

- 1) Strengthen public health surveillance to ensure rapid detection of unusual outbreaks;
- 2) Strengthen epidemiological capacity to investigate and control health threats from terrorist events;
- 3) Enhance public health laboratory capability (both chemical and microbiological) to identify agents most likely to be used in intentional release events; and
- 4) Develop/coordinate communications with local government agencies and the general public to disseminate critical information and minimize unnecessary fear.

Public health agencies need improved public health infrastructures that can detect intentionally caused disease outbreaks early and provide treatment. An observant, well-trained local health official should recognize that something out of the ordinary has occurred and alert public health authorities through prearranged communication channels. In many instances there is only a short window of opportunity to determine the following:

1. That an attack has occurred;
2. To identify the toxicant/bioagent;
3. To prevent further exposures; and
4. To mitigate the event where possible

First and foremost, local communities must have a coordinated response plan to a possible terrorist attacks. These response plans should include law enforcement, medical first responders, and public health officials. While the FBI has jurisdiction for terrorism response, local communities must have trained personnel available for rapid response. If chemical or bioterrorism is suspected, the local emergency response system should be activated.

In the event of a bioterrorist attack, rapid diagnosis is critical to the immediate implementation of prevention and treatment procedures. Future events could involve organisms that have been genetically engineered to increase their virulence, possess antibiotic resistance, or evade vaccine-induced immunity. Due to the fact that many of the bioweapons are currently not major public health problems in the United States, there is a limited capacity to diagnose them. Therefore it is important that the local health departments work with state health laboratories to increase the capacity to identify possible disease agents.

Local health departments should have the capacity to detect outbreaks of food-borne diseases caused by deliberate contamination. The early detection of these types of disease outbreaks can help avert possible widespread consequences.

In this regard, CDC's Epidemiological and Laboratory Capacity (ELC) program can help local health departments develop the skills and resources to address whatever infectious disease challenges may arise. One of the specific aims of the ELC program is the development of innovative systems for early detection and investigation of outbreaks.

Early Detection

A sentinel disease detection system involving local networks of clinicians and health providers should be established. In this way the medical community will be alerted in a timely manner so that health workers can identify disease threats. Additional resources to aid the sentinel process should be established with local academic, government, and private sector organizations.

Rapid Communications and Information Access

In the event of an intentional release of a chemical or biological agent, rapid and secure communications will be crucial to ensure a prompt and coordinated response. Each hour's delay will increase the probability that another group of people will be exposed, and the outbreak could spread both in number and in geographical range. The establishment of a Health Alert Network (HAN) will result in a well-developed communication, information, distance learning, and organizational infrastructure for a rapid-response to chemical and bioterrorism. Such a network would incorporate the following:

1. Continuous, high-speed connection to the Internet;
2. Broadcast communications;
3. Satellite- and Web-based distance learning.

National Pharmaceutical Stockpile (NPSP)

Once the cause of a terrorist-sponsored outbreak was determined, specific drugs, vaccines, and antitoxins might be needed to treat the victims and to prevent further spread. Appropriate medical supplies may not be readily available to local responders, or in the

quantity needed, since many infections are uncommon causes of disease in the United States. Therefore local health departments should avail themselves of the CDC-sponsored stockpile of pharmaceuticals that are available anywhere in the continental U.S. within 12 hours.

About the Author

Dr. Wagner is a noted scientist with years of experience in environmental toxicology and medical parasitology. His experience includes "hot zone" assessment of health effects during catastrophic disasters, such as train derailments. He is an Assistant Professor of Environmental Health Science at Salisbury University, Maryland. He also teaches at FEMA's National Emergency Training Center, Emmitsburg, Md., and the Emergency Assistance Center, Mt. Weather, Va., with specialty areas that include chemical and biological agent releases and exposures.

* * * * *

Fire Departments, Emergency Medical Services, and Emergency Management Agencies

By Timothy R.S. Campbell

The events of September 11th, 2001, will all ways be etched in our minds as the day we all awoke to the true face of world terrorism. It will, however, be remembered as well as the day Americans realized what the fire and emergency medical services risk in performing their duties. The days that followed showed what emergency management is in its broadest sense.

Fire Departments have historically been the first responders to incidents of disaster and other major emergencies at the municipal level of American government. In recent years, Emergency Medical Services, either as part of the fire service or as a third service, have joined the response panoply. With the integration of public works agencies into disaster response, the need for coordination and combined planning helped raise the civil defense/emergency management component into the role of governmental coordinator of responses.

The fire and emergency medical units that responded to the World Trade Center did so as the first organized team response. Not to take anything away from the New York City and Port Authority police or the building fire, security, and maintenance staff, but they responded as individuals. The fire and Emergency Medical Services units also brought the first complement of tools and personnel protective equipment.

This is how fire units have responded since Roman times. An organized group, operating under some form of disciplined command, arriving equipped with tools to handle the event. These units were organized primarily for community protection, and generally operated from geographically dispersed stations around the community.

Fire departments have also had to deal with the problems produced by the introduction of new technology into society. Often this occurred as a result of an incident that cost fire service lives. As the science and art of firefighting grew more complex, fire departments added new skills and equipment to their inventory. This ability to change allowed fire departments to adapt to the new missions of vehicle rescue, hazardous materials incidents, and emergency medical care. New forms of breathing apparatus and personal protective turnout ensembles allowed fire fighters to get in closer to the incident and still be able to operate safely.

In addition, the structure of the fire department has allowed the creation of specialized units within the community. Organized into engine or ladder or rescue or hazardous materials units, the ability to deploy mission specific teams has provided the most efficient use of personnel and equipment resources.

Additionally, the fire department command structure has provided the basis for an on-scene command system that manages all elements of the situation at the incident scene. Validated through a series of large wildland fires that required response by agencies from the federal state and local governments, it has been adopted for use at hazardous materials incidents, wildland and urban searches, and even large special events. It also can seamlessly interface with the community emergency management system.

As we look at the American fire service, we see that the departments and the system generally are the same from large urban center to suburban communities to the rural and frontier environment. Major wild land fires in the western parts of the United States have shown the ability for fire units from local, state, and federal agencies to deploy in a multi-region and multi-state response when required.

The difference is sometimes in the number of fire department stations and staffing in mid-sized communities. Here, the requirements of large fires and possible terrorism incidents will require mutual or outside aid for incidents that larger jurisdictions might handle on their own. These agreements will be executed between the elected bodies and managers rather than directly between the operating fire departments. The agreements may include the provision of automatic aid that responds on initial dispatch or for the support of specialized units such as hazardous materials teams. Often the assistance will cover non-fire service assists such as Emergency Medical Services and police as well.

Beginning in the late 1960s the United States saw the formation of specialized pre-hospital medical care units that replaced the previous simple ambulance transport often offered by private sector organizations. These extensions of the care available in emergency departments of local hospitals were provided by governmental and private sector sources. Trained crews would respond to the scene of an emergency and assess the patient and then initiate care before loading and transporting to the hospital.

Seen as operating under the guidance of a licensed physician, these units initially operated under direct radio voice oversight from medical personnel at the hospital. As the services of these specialized units spread across the country, there arose situations where radio communications could not be reliably established and units began to operate under standing orders or protocols.

Sometimes these emergency medical services became the sponsors of specialized teams that were fielded by fire departments elsewhere. These included wilderness and vehicle search and rescue operations and sometimes marine or hazardous materials units. In some communities where the fire department did not provide the emergency medical care service, the fire units provided a first responder service it provided initial patient care and stabilization. This often occurred in communities where emergency medical services units were not overly sufficient for peak periods. In others, it was seen as a way to involve units that were becoming under-utilized as fire incidents dropped in number due to active fire prevention and code enforcement.

Emergency medical services units sometimes became involved in providing more routine medical care activities such as blood pressure screening or health living education or cardio pulmonary resuscitation training. In other communities, the units became overwhelmed with calls for service as access to primary care became restricted and citizens began to view the local emergency room and ambulance as sources for routine medical care. Another area of concern for emergency medical services groups was in the planning and training for events that would produce large numbers of casualties.

The nature of emergency medical services and the fire service meant that the units were often called to the same incident to provide their services. Here, the beginning of modern multi-disciplinary, inter-agency operations can be seen. In the past, units may have been at the same event, but provided their services almost in isolation from the other services present. The integrated actions of the fire and Emergency Medical Services units often led to inter-agency planning and training. This was enhanced when Emergency Medical Services units were based in fire stations, even when operated by another entity.

While America has had a civil defense system since the early 1950s, it was not until the development of the National Governor's Association report on emergency preparedness in the late 1970s that modern emergency management began. Many states in the U.S. had been using their civil defense assets for non-war related emergencies in differing degrees, but there was no real consistency. There was so much of this going on that some authorities were concerned about the level of war-related preparedness that the civil defense federal funding was supposed to ensure.

The results of the incident at Three Mile Island nuclear generating station in 1979 confirmed the need for detailed multi-agency planning and training for disasters and emergencies. With changes in federal laws, many states evolved their civil defense programs into all hazards emergency programs. They ranged in complexity from central planning and training focuses to organizations that deployed fleets of emergency equipment to local jurisdictions. During the 1980s there was still a major concern about war-related issues, but with the fall of the "Iron Curtain" focus shifted to natural and man made hazards.

Experiences dealing with the hurricanes, tornadoes, and storms of the late 1980s and early 1990s confirmed what had been learned during hazardous material incidents during the safe period. Major efforts put into active inter-agency planning followed by inter-agency training and exercises, combined with good communications system and coordination centers, provide the community with the best ability to manage the consequences of the disasters. They also showed that efforts to reduce the impact of a disaster would produce significant savings in lives lost or disrupted and in damages and costs incurred for response.

These conclusions were reinforced by after-action analysis of the increasing incidence of terrorist related events. The 1993 World Trade Center bombing, the 1995 Tokyo Subway Sarin attack, and the 1995 Murrah Office Building bombing all showed the benefits of integrated response and the problems that occurred when components of the

system were not coordinated. These events showed that most communities had the majority of resources required for handling or preventing a terrorist incident.

What was needed was to identify the areas where capability was lacking and to develop a plan to fill these gaps. Examples include increasing the capability of hospitals to decontaminate patients or for hazardous materials teams to detect chemical warfare agents or training public health laboratories to assess biological threats. Many of these efforts would build on capability all ready in place for every day emergencies in chemical plants or facilities using radiological materials or in managing epidemics.

For much of the late 1990s, efforts were made to fill these needs. Federal and state training programs increased the number of offerings of courses relating to terrorism and weapons of mass destruction. Funding programs were provided to begin to acquire the specialized personnel protective and detection equipment needed. Plans were reviewed and procedures developed for an attack involving large explosives or chemical, biological and nuclear materials.

Yet on Tuesday, September 11, 2001, the United States suffered its largest loss of life to a terrorist attack that used jet fuel and impact to bring down the World Trade Centers. Fire, Emergency Medical Services, police, and public works personnel from the involved local governments, along with private sector security and safety personnel, supported by emergency management and communications staff, responded and tried to stabilize and handle the incident. Soon thereafter, a series of anthrax hoaxes and actual attacks struck across America and then around the world.

This is evidence that the governmental and public safety personnel of the United States must begin to think like the terrorist in planning and training for possible attack. We must understand that our responders are targets. We must realize that our cities and homes are targets. We must analyze our way of doing business and determine what actions and capabilities are useable during an attack.

We must remember that our responders will attempt, within the capabilities of the equipment issued and training received and policies in place, to effect change in the event that reduces the loss of life or rate of injury. This is what the fire service has done since Roman times and has been adopted as a mission by emergency medical and emergency management personnel as they serve our communities

About the Author

Timothy R.S. Campbell is a consultant on emergency services and public safety. For 20 years he was director of emergency services for Chester County, Pa., an agency serving 73 cities, 123 public safety agencies, and more than 400,000 citizens. He serves as an instructor for Integrated Emergency Management courses at FEMA's Emergency Management Institute, Emmitsburg, Md.

* * * * *

Emergency Medical Response to Terrorist Incidents and Hoaxes

**Deputy Chief James G Fogarty
Emergency Medical Services
City of Clearwater Fire Department
Clearwater, Fla.**

In the days since the September 11th terrorist attacks many, Emergency Service Agencies are rethinking their preparedness and operational approaches to reports of biological substance scares as well as how they might better handle the more credible threats within their communities. Moreover, terrorist events of every sort have garnered a new standing in the hierarchy of readiness. Now, along with the inevitable traffic crash and heart attack patient, stands the real possibility of a subversive event that will land inside your community.

Only a short time ago EMS providers worked through such issues by using existing resources and protocols with slight modifications, which seemed to suffice. Terrorist type calls were infrequent and almost always bogus. In many cases a response for terrorism was a matter of working through the issues like a detective considering the tangible proof that would define the likelihood for significance event to have occurred.

Many situations are breaking new ground in an area that until now had no empirical cases to review to test assumptions and effectiveness. There have been many hoaxes of substances that ultimately failed to show any pathogens, but unlike other medical events such as heart attacks or trauma, there are but few methods to choose from with the terrorist event. Many occasions where information and understanding was poor, full-scale hazardous material type responses garnered both accolades and criticism of the responders. The occasional sentinel event where a bomb would explode happens to fit well into the normal mold of response and is more straightforward in the response approach.

Although a terrorist event is never routine, managing such events here-to-fore became a function of scale of operations with larger events simply requiring more resources to deal with them effectively. Dealing with extreme events, such as what occurred on September 11th has always been thought of differently. It has been assumed that such events are of such magnitude that no level of rational preplan could adequately deal with such issues. Perhaps this is partially still true today, but clearly operational readiness must adapt to our new reality.

What follows is a discussion suggesting some operational changes that might be considered in implementing plans for future dealings with bio-terrorists events. Although written from an operational perspective, key decisions and support are needed at a more strategic and administrative levels to allow the carry through into day-to-day operations. There is much to learn, as we become both teacher and student in the face of this new enemy.

Emergency Medical Services

In its most basic definition, the Emergency Medical Services (EMS) operating in the United States provide a mechanism for an immediate response of trained persons to the public's self-defined request for help. We operate under a premise that someone(s) in the community has immediate need of medical care that cannot wait or perhaps cannot access normal clinical health care channels due to a potential life threat. Perhaps a moribund situation exists so a call for assistance enters a system of response beginning with a call to 911. EMS maintains response assets necessary to provide these essential services in the streets and living rooms of the community.

Agencies prepare by obtaining equipment and supplies they expect might be needed based upon the typical calls for service within a community. They also prepare by certifying personnel in areas they can expect to manage clinically. Medical calls such as cardiac events and traumatic injury each have developed methodologies for treatments as well as specialty destinations to effectively deal such occurrences. Treatment methods known as "**Protocols**" or alternatively "**Treatment Plans**" are designed to allow the rapid application of treatment tactics in a time compressed and information poor environment. The process begins with general interventions and moves more aggressively once specific information is obtained. By administering tests or soliciting information via history taking, the gathered information fine tunes the care given and provides for the successful outcomes desired by patients.

Preparing EMS resources in anticipation of dealing with terrorism of every sort then becomes a mix of "**Operational Update**" and "**Strategic Change.**" Compared with other medical events, a terrorist attack may go undetected throughout the incubation period where it can most effectively be managed. Operational necessity requires early detection, but as we have witnessed over the last few weeks, a degree of on-the-job learning occurs as we face situations not previously managed. EMS agencies, extrapolating from known response methodologies such as Haz-Mat protocols, have dealt with issues of potential biological exposures (Anthrax) as well as the very unlikely exposure situations involving routine mail delivery (hoaxes). As is often the case in Emergency Services, effective interagency coordination has provided a framework from which we can now build to better transition our communities in dealing with terrorism events. The review of this initial framework we now have, plus the addition of shared information, makes this rapidly unfolding topic one we can deal with effectively.

Today there exists an immense body of knowledge on subjects surrounding biological terrorism and other forms of terrorism. Use any search engine on the Internet to clarify the point. This knowledge grows daily so health care providers must not only have access to these information channels but they also need to know how to utilize the information to best advantage. Medical knowledge itself is updated frequently so staying abreast of current trends is nothing new. How to best treat Anthrax, speed of diagnosis, and vaccine strategies all are undergoing review as we learn from existing case studies.

Specific Actions

Processing Information

Today, there are literally thousands of resources readily available for researching the methods and approaches in dealing with terrorism. From a practical sense, the amount of information is overwhelming to a casual observer. Sifting through this information and focusing upon only those choice pieces of information that are now relevant to the issues at hand is a **key** factor in preparing for and/ or responding to emergency situations such as terrorism

Broadband high-speed access

Each Healthcare agency needs **broadband high-speed access** channels. The extent of this access can be as far reaching as within each response unit but at minimum each administrator and point of entry for patients must have data entry terminals for rapidly entering information into its data systems. We must also maintain treatment plans, expert resources for referral on lesser know disease entities, and decision-support systems to help deal with multivariable health care issues.

Standard data set

The time is long past for a **standard data set** and interchange within the healthcare system. The Centers for Disease Control has in place several standard data definitions for reporting and tracking reportable diseases. Health Alert Networks have been field-tested in San Diego, Atlanta, and Monroe County, N.Y., proving the feasibility of real-time monitoring of local health conditions through sentinel sites at Emergency Departments. It is well within the current technology to spot increases in symptomatic patients within hours of arrival at a healthcare facility. Admittedly this model is still reactionary as it identifies illness as symptoms develop and often waiting until after symptoms appear is not ideal in administering effective treatment. Nevertheless, it is a necessary monitoring tool. It is a place to start and well within the resources that exist today. We must take full advantage of existing data standards that are utilized daily, such as International Classification of Disease (ICD 9) codes or Diagnostic Related Groups (DRGs). There is a vast array of demographic data from the census bureau, and community data from such sources as the property appraisal system. Any individual that has ever been hospitalized, has medical insurance, or qualifies for Medicare or Medicaid has a medical file in electronic format. Interconnecting these formats is a matter of technical conversion.

I acknowledge there are issues of security and confidentiality that must be addressed. These issues are not new and can and must be dealt with by those that can best shape the issues from a legal and practical standpoint. Of course we must preserve our rights, yet at the same time we need access to standardized and unheeded information flows. Implementing Standard Data Sets will provide increased advantage in dealing with the health care issues surrounding biological terrorist events. I do not propose more information; we already have volumes of the data. I am espousing an ease of use across

the health care networks. This ease of use starts with standard data sets then continues with focusing of data.

Information must be available when and where it is most effective and more importantly not lost among what is not relevant. Information itself is not powerful; it is what you do with the information that is powerful. It remains useless unless acted upon.

Communications

Today an emergency response requires instant and multifaceted communications networks that are reliable and flexible. Healthcare systems generally have solid infrastructure in place that consists of various radio and phone based systems. Data uplinks have already been described and must contain electronic mail systems and remote conferencing capability. These items are most likely present on existing systems, although not often utilized. It is this lack of routine use that makes them less effective and less likely to be considered in times of crisis.

Redundant phone systems

Redundant phone systems, both analog and digital, phones should exist as well as wireless. Digital systems work well and the many features allow for the needed mass communications capacity of today. Analog is needed since it is not as reliant upon the computer control networks to make it function. Wireless has become a standard tool for field operations and has performed well even under extreme conditions and volumes. I am saying more than “buy some phones.” This preparation step involves a comprehensive communications plan that can be rapidly expanded as the situation warrants. An ability to increase the number of dedicated wireless phones within the health care system should rank high on the “To Do” list. Contracts with phone service providers can provide the needed connectivity for a very modest cost while preventing the unused capacity costs that would exist with continuous high numbers of phones. Cooperation on behalf of the phone industry is high and most areas enjoy the rights of public safety entities in dedicating priority phone service in time of declared disaster. Those phone number lists of all your priority phones should also be on your “To Do List” and should become a semiannual update ritual. Such rituals not only keep lists current but also remind both service provider and your own agency of this process, which makes it more likely to be taken advantage of if the time comes

Broadcast fax capability

Broadcast fax capability can be part of the phone systems or stand alone networks. These systems allow quick dispersal of information to a wide geographical area. These systems have seen use in natural disaster situations as well as regular public service announcements. They allow rapid delivery of printed material within the community separate from other electronic systems

Networking Alliances

Network of contacts

Develop a network of contacts for your agency. This is not career advancement advice from the latest motivational speechwriters, but a key tool in the preparation process in dealing with crisis. Consider the networks at work within a trauma center as an example of how effective they are in crisis management. The emergency physician has a vast array of on-call specialists to bring into the treatment plan for traumatic injury. Using expert knowledge for the local area treatments can be provided in less than one hour for situations of a very complex nature. Effective approaches to biological events should mimic this course in both preparation and response. Many key benefits results from this simple, low cost preparation process such as:

- A sense of trust develops within those consulted
- Confidence created within those that are part of this process and know the aspects of expert help that can be brought to bear on whatever issue presents
- Easy access by the direct and personal friendships that develop

So whom do you invite to be part of your network? You can include anyone within your community that fulfills a role in handling complex health care issues. Consider how you would deal with a large-scale event such as an aerosol release of a biological agent: for example, Anthrax. Many widespread tasks need to be performed to deal with the release, some of which are not clearly defined. For example, the community must understand the issues surrounding the infection of airborne disease and to do so must trust the people in charge. The lab technician is the first person to know of the tests results and must know how important those results be reported quickly and accurately and who they must be reported to. These and hundreds of other tasks become easier with prior contact with key individuals throughout your community. Your list of network contact should include:

- Police and Fire Department
- Medical Director
- Emergency Management
- Emergency Room Managers
- ER physicians
- Public Health Unit
- Lab Manager
- Infection Control Officials at each Hospital
- Pharmacy Manager
- Data Control/Information Services

This is not hard to accomplish. Next week hold a coffee meeting with one objective, to get to know each other. Calling “Pete” from Infection Control at the local hospital at 3:00 am tends to be much more productive when we know each other.

Remember: People solve problems.

You should plan to leave with no less than two ways to contact each individual and preferably also an e-mail address. Provide them your contact information and then, as a test, contact them on your very next suspicious powder hoax to bring them into the plan during a relatively controlled event. Once they understand and feel part of the team, the benefits will start to appear. This may appear to be fundamental in the context of terrorism response, but if you review how the events unfolded in Florida and New Jersey it was these small details that produced the effective action required at the time. The value of this should not be underestimated.

Training

Under the assumption of limited resources, how should our time and money be allocated? Many agencies find it difficult to devote the time and money needed to properly address all that is needed to prepare and then to stay current with the infrequently used skills such terrorism issues. Skills not frequently practiced are soon forgotten. Our system of public health has long been held to constraint decisions. The likely starting point for these types of decisions flows from your own system's vulnerabilities to attack. Secondly, they can flow from the combination of likelihood of occurrence and probability questions, and the impact should an event occur (quantifiable impact of an event's occurrence). Some terrorist events will be very rare indeed, but the consequence should one occur are too profound to ignore, despite infrequency. You can rationally distribute existing training budgets and make a case for increased need and have a defensible plan to sustain the levels of readiness supported by the community.

Surveillance

Every practitioner in medicine must know the basic tenets of disease surveillance. This includes definitions and nomenclatures that are specific to this discipline. Most medical technicians do not have even a basic understanding of epidemiological constructs. Reportable diseases, the process for reporting them, and how feedback is provided to the community are other key elements of this surveillance knowledge. Public health can provide a primer on this and other topics through existing training channels. Emergency responders must understand various concepts in epidemiological medicine. CDC, through the local office of public health, can provide excellent and very low cost training programs on epidemiological issues that each practitioner should attend.

Special Care Plans

Emergency medicine deals with *time critical events* framed in *an information poor* environment with dire consequence in the absence of, and sometimes in spite of, the proper sequence of interventions. Protocols now exist for the preventative management for significant exposure threat for many diseases. The need for speed and widespread application of terrorist related medicine is new and has only few instances of empirical cases that we may review. The actual efficacy of such protocols remains to be reviewed. Medical providers must stay informed regarding the latest trends in **testing and treatment** methods, prevention strategies, and population based reportable diseases as they evolve.

They must know the accuracy of those reports and how their involvement in health care obligates that they be part of the reporting process.

Reports are provided weekly on-line at the CDC website, or you can download the Morbidity and Mortality Weekly Report. But it is imperative that methods be developed to sift through this information in an effort to focus upon the relevant, then act from a standpoint of facts and data. In order to filter through the vast information stores of Public Health and other agencies, expert decision support systems are needed. Strategic change in the preparation and deployment of medical resources (response) must improve to limit any spread of communicable disease and manage those with infectious diseases.

Response agencies now apply existing hazardous materials models to incidents that involve unknowns. Haz-Mat teams have the equipment, training, and necessary contacts to mitigate such events. Although several un-necessary decontaminations have taken place, requests for service to deal with unknown substances are taxing their resources while providers seek a more efficient approach to such issues.

Confirmation tests

Fast yet reliable tests are currently available for cardiac patients. An enzyme marker test can identify persons having heart attacks easily. Using portable sonograms we can peek inside a body cavity to identify a distressed child in sufficient time to intervene successfully. Microbiology is advancing in the area of confirmation tests but remains delayed. The task is to provide confirmation test tools similar to those used in emergency rooms for rapid diagnosis of conditions. We must have tests faster than a culture plate taken from a swab and we must become more accurate than microscope viewing of a stained slide. Standard practice must be updated quickly. There has been progress as we observe the advances in screening for such diseases as Hepatitis C, which only a few years went from an unknown entity to one that could be identified using a blotter sample. EMS has also had some experience with HIV exposures management. Programs exist that provide critical source patient information to an exposed individual in minimal time, thus allowing treatment to be directed from factual information sources rather than probabilities.

Add to the “**To Do** List” the ability to obtain rapid test tools for those disease specific entities that predominate a terrorist’s laboratory. The lists of diseases will undoubtedly change over time, but our approach will not. We need the ability to test for a piece of critical information, the presence or absence of disease and to do so quickly and portably. With that information we can act, without it we can also act but much less efficiently.

(continued on next page)

In Conclusion

Hospitals

- Review all relevant disaster response plans and assure appropriately designated staff are familiar with their content and strategies.
- Establish internal and external lines of communication. Assure that medical staff are aware of the need to report suspicious cases of illnesses to public health authorities, and are familiar with who these authorities are. Have in place dedicated staff, phones, and fax machines to support rapid reporting.
- Hospital leaders should establish collaborative strategies for communicating with neighboring hospitals, civic leaders, and public health authorities.
- Quantify pharmaceutical and antibiotic supplies, both at central and satellite facilities. Routinely update this list.
- Assess routine staffing and emergency call-up plans and assure that these are supported with communication and transportation strategies. Update the roster of essential personnel.
- Maintain ongoing primary and redundant communication systems.
- Assure that appropriate health care professionals (e.g., emergency dept and urgent care dept personnel, infection control and infectious diseases professionals) are aware of the importance of reporting unusual disease presentations, disease clusters and atypical patterns of hospital use and know the mechanisms to do reporting.

Physicians

- Develop an increased awareness of the ongoing threat of bio-terrorism.
- Become familiar with and develop a working knowledge of the most likely and dangerous pathogens as viewed by the CDC.
- Become familiar with relevant lines of communication, and important and emergency phone numbers (hospital epidemiologist, state epidemiologist, local health department [may be city or county]), and the CDC emergency number.
- Monitor disease patterns and patient volumes in clinics and offices. Immediately notify the appropriate authorities if you suspect an unusual event or need medical guidance.
- Patients can also be referred to the CDC public inquiry phone number regarding information about infectious diseases and bioterrorism preparedness response efforts. Have referral numbers for mental health and support services as needed.
- The Center is aware that a number of physicians have received requests for prescriptions for antibiotics to be used in the event of a bio-terrorist attack. It should be known that Centers for Disease Control maintains a National Pharmaceutical Stockpile of large quantities of antibiotics and vaccines that could be distributed in the event of an epidemic brought on by an act of bio-terrorism.

Emergency Medical Services

- Ensure that leaders are generally familiar with what a bio-terrorism attack might demand of civil authorities, and what resources are available to meet these demands. Identify and, if feasible, meet with public health and medical experts who might provide guidance to key decision-makers during a public health emergency.
- Put in place primary and back-up communication systems to assure that civil authorities can contact key medical, public health, and emergency response workers 24 hours a day, 7 days a week in the event of a public health emergency.
- Assure that civil authorities can quickly broadcast emergency messages, health alerts, and educational information across multiple media including radio, television and web sites. If older civil alert systems, e.g. air horns, etc. are available, educate the public regarding their possible use and meaning.
- Identify existing gaps in linkages, coordination of response and communication between hospitals, public health agencies, and emergency response workers.
- Develop transportation plans that facilitate movement of emergency vehicles, entrance to and egress from hospitals and care centers, and rapid deployment of essential health care workers from their homes or off-site locations to primary hospital and health care sites.
- Designate a dedicated point of contact to receive information from medical and public health agencies in the event of a bio-terrorism attack.

Public Health Agencies

- Local and state public health agencies should collectively review bio-terrorism response plans. Attention should be given to assuring the integration of response plans, including mechanisms for sharing resources and personnel as needed.
- Syndrome surveillance procedures should be put in place to monitor and detect atypical disease presentations and clusters. Both passive and active surveillance systems should be examined and refined across public health agencies and with reporting sources.
- Establish and maintain capacity to accept reports of unusual disease events twenty-four hours a day, seven days a week. Assure systems of continual, bi-directional communication between public health agencies and hospitals under their purview.
- Appropriately trained disease investigation staff should be available for immediate mobilization and deployment as needed. Staffing levels should be reviewed and plans put in place to determine non-urgent public health functions and clinics should it be necessary to pull additional clinical and field staff for urgent investigation activities.
- Assess communication systems, including procedures for immediately contacting public health and political leaders. Systems should be assessed to assure that appropriate authorities could be contacted at the outset of an emergency. Mechanisms for maintaining ongoing communication, including pagers, cell phones and wireless email systems, should be assessed and tested. All staff that provide on-call and disease investigation response and decision-making should be adequately resourced for 24/7 communication.

- Hold regular meetings with all appropriate government and non-governments agencies and organizations to continually review and refine plans.

About the Author

Chief Fogarty heads the Emergency Medical Services of the City of Clearwater Fire and Rescue Department in Pinellas County, Fla. He has more than 25 years of experience in Emergency Services. He is a graduate of the Executive Fire Officer Program at the National Fire Academy and holds degrees in both Emergency Medical Services and Fire Administration. As an adjunct faculty with FEMA since 1993, he helps conduct Integrated Emergency Management Courses for communities throughout the United States.

* * * * *

The Challenge of Cyberterrorism

Excerpted from *A Survey of Terrorism*

By Robert T. Thetford, J.D.

© September, 2001 by Institute For Criminal Justice Education, Inc.

P.O. Box 293

Montgomery, AL 36101

www.ICJE.org

Used with permission

The first known cyberattack occurred in 1998, and was a limited attempt by Tamil guerrillas to swamp Sri Lankan embassies with e-mail, according to U.S. officials.ⁱ This attack may have been crude and ineffective but it set the stage for more serious cyberattacks in the future.

While the use of "hacking" or more appropriately named "cracking" techniques have been used by unscrupulous individuals (mostly teenagers) for over 10 years in the United States to gain unauthorized access to computer systems, the use of these techniques by states or organized groups to deliberately disable or destroy the computer systems and infrastructure of their enemies is a relatively recent phenomena.

In 1999, an Associated Press report detailed an apparent coordinated electronic attack by the Chinese on Internet web sites operated by the Falun Gong meditation group.ⁱⁱ The report stated that at least one "hacking" attempt appeared to have been traced back to a Chinese national police bureau in Beijing.

Attack Methods

The vast majority of electronic attacks involve amateurs who have copied programs from the Internet or from their friends. Armed with these programs, the attackers, most of whom are still in school or are school age, can and have caused damages running in the millions of dollars. Other hackers attack computer systems merely for the thrill of the attack itself and leave "calling cards" as to their visits, or simply do it in order to brag to their friends.

Often a hacker will gain access and open a "back door," a separate entry point to the computer system, which allows the hacker to enter the system undetected at will and provides a sense of ownership over the system. Knowing that the system is his for the taking provides a feeling of absolute power, an emotional state that is frequently necessary for the hacker's self-esteem.

A further measure of control involves inserting a "Trojan Horse" into the system files. This is a program which a system accepts, usually because it is not detected or because it is recognized as a benign file. Trojan Horses often contain malicious code in the

form of “Logic Bombs,” which are programs residing in a system without interfering with the system operation until activated through the passage of a certain amount of time or the occurrence of a certain event. Upon activation, the Logic Bomb may do anything its designer has programmed it to do, including destroying the system files or spreading viruses.

A virus is by definition a program that reproduces itself. It may destroy or alter data or use system memory, or it may simply reproduce itself, but it generally stays within the computer system. Worms are similar to viruses in that they copy themselves over and over, generally degrading system resources, but they are designed to reproduce across computers systems (for example, through e-mail) and are therefore potentially much more dangerous. Even the most innocuous of these are vicious, however, and cause serious problems for computer systems. Although the total number of viruses (and worms) is unknown, one leading manufacturer of anti-virus software advertises that its program protects against over 50,000 viruses.

Just how much damage do they cause? The latest estimates of one of the more recent worldwide virus, the “Love Bug,” which originated in the Philippines and quickly spread to both Europe and the United States, indicate that the damage to computer systems may have run as high as \$10 billion.ⁱⁱⁱ This virus was allegedly created by college students as a research project. Imagine what a terrorist group could accomplish with determination and a fundamental understanding of computer technology.

A growing form of cyberterrorism common in Europe (and beginning to be used in the United States) is Cyber-extortion. The typical scenario in this criminal activity occurs when an individual or group threatens to destroy, publish or sell data files of a company if a certain fee is not paid or an action by the company is not undertaken. Often the extortionists will have gained entry into the system files and left a “calling card” in order prove the validity of the threat. Companies frequently accede to the demands rather than report the threat to the police because they understand the damage that can be done and also because they are afraid of the effect on their customer or client base if a security breach of client data becomes publicly known.

Perhaps the most devastating computer attacks occurring from 1999 to 2001 have been “Denial of Service” (DoS) attacks or “Distributed Denial of Service” (DDoS) attacks, often caused by “Mail Bombs.” In a DoS attack, a computer (or a group of computers in the case of an organized attack) is directed to flood the target system with e-mail or requests for information. A DDoS attack accomplishes the same goal using captured, third party computers. In this type of attack, third party computer systems (called Zombies) are in essence hijacked and used to flood the target system with requests for information or e-mails, thereby totally overwhelming the target system and shutting it down for commercial traffic.

DoS and DDoS attacks cost private industry only \$77,000.00 in 1998, but cost an estimated \$8 million in damages during the first two months of the year 2000 alone.^{iv} In the United States, Mail Bombs have been used by eco-terrorists to tie up their adversaries,

with over 50,000 e-mails being sent in 1998 to a Swedish facility that conducts research using monkeys.^v The DoS attacks of the last few years have caused considerable damage to major U.S. Corporations, yet they appear to have been directed by teenagers, not organized terrorist groups. The magnitude of damage which could be caused by a well organized and orchestrated attack carried out simultaneously from numerous locations is staggering to computer security professionals. Richard Clark, a National Security Council analyst, advised in December, 2000, that the U.S. government believes tens of thousands of innocent computer systems may have already been turned into "Zombies" that hackers could use to cripple the Internet.^{vi}

The Targets

Most experts feel that military installations, power plants, air traffic control centers, banks and telecommunication networks themselves are the most likely targets for a cyberterrorist attack. Other targets include police, medical, fire and rescue systems, which could easily be damaged, along with Wall Street brokerage firms and water/sewage systems.

During the Gulf War in 1990, a group of Dutch hackers calling themselves "High Tech for Peace" approached diplomats in the Iraqi Embassy in Paris. The hackers offered to disrupt the electronic network handling logistics messages between bases in the U.S. and U.S. military units in Saudi Arabia if the Iraqi Government paid a fee of \$1 million. The Iraqis refused, but in reality they probably should have accepted the offer. A study later showed that 25 percent of the electronic messages coming into Saudi Arabia were uncoded and were totally vulnerable to interception and disruption. Had this offer been accepted the U.S. military supply lines would have been severely affected.^{vii}

In a recent briefing before the U.S. Congress, George Tenet, Director of the U.S. Central Intelligence Agency, said at least a dozen countries are developing programs to attack other nations' information and computer systems. China, Libya, Russia, Iraq, and Iran are among those developing such systems. Additionally, a new classified National Intelligence Estimate reports at least one instance to date of active cybertargeting of the United States by a foreign nation.^{viii}

In 1996, a Swedish hacker, moving through cyberspace from London to Atlanta to Florida, rerouted and tied up telephone lines to 11 counties, put 911 emergency service systems out of commission, and impeded the emergency responses of police, fire, and ambulance services.^{ix}

While many of the foreign cyberattacks grab the headlines, domestic cyberattacks are increasing at an alarming rate with the number of pending FBI cases involving cyberattacks increased from 128 in 1996, to 1,154 in 1999.^x

Nor are the cyberattacks limited to business and educational establishments. In 1998, the FBI executed search warrants on the homes of two California high school students after determining that they had gained entry to a number of government computer

sites. Their hacker assaults on the Pentagon, NASA, and a U.S. nuclear weapons research lab were described by a deputy defense secretary as "the most organized and systematic attack" on U.S. computers ever discovered. To make the Pentagon attack hard to trace, the hackers routed it through the United Arab Emirates. They were directed in this attack by a teenage hacker in Israel.^{xi} While all of those involved were arrested, in a typical case little punishment is imposed on teen hackers due to their age. The situation is even more complicated with the discovery of a teenage hacker in another country. In most recent situations, the United States has left the prosecution of teenagers to the discretion of their home country, even if extradition treaties would allow prosecution here.

The vulnerability of technologically advanced countries such as the United States to cyberattacks became acutely apparent through government studies of the Y2K problem in 1999. It was discovered that the "triad" of electric power, banking, and telecommunications was especially susceptible to cyberattacks because of the heavy use of computers in these industries and the mandated use of telecommunications to link the computers. The interdependence of these industries makes protection against electronic intrusion vital to the continuation of an advanced society. When it is understood that without telecommunications, both banking and electric power will fail; that without electric power, both telecommunications and banking will fail; and that without banking, the economic infrastructure of a country will fail, then the magnitude of the problem can be seen.

James D. Kallstrom, former chief of engineering at the FBI laboratory in Quantico, Virginia, in discussing the possibility of computer network based cyberattacks, advised:

We are using the efficiencies of technology and the Information Age to control everyday things like traffic lights, 911 systems, the environment of buildings, the communications network, and the power grid. We even control the water supply with computers. We are doing more and more things like that. In the old days...Fort Knox was the symbol of how we protected things of great value: we put them in buildings with thick walls and concrete. We put armed guards at the doors, with sophisticated multiple locks and locking bars. We could even build a moat and fill it with alligators.... Today [with] things of that same value, you wonder if some teenager is going to go in on the phone lines and steal it all. We are not equipped to deal with those issues both in the government and private industry.^{xii}

Brian Jenkins, an analyst at the Rand Corporation, a U.S. think tank, expressed a similar view:

In the past, when terrorists wanted to conspire, they usually had to get together and meet in person. Nowadays, they can take to the Internet and find like-minded believers, even if they don't know them already.

We have not even begun to comprehend the consequences of the Internet to create an army. Their ability to communicate with one another, to find reinforcement -- even justification -- for crazy views is of extraordinary importance.^{xiii}

The Future

It has been estimated that 90 percent of all criminals in the U.S. are now computer literate.^{xiv} This percentage would indicate a dramatic increase in the number of computer crimes overall, including the use of computers for terrorist acts. As the computer literacy of terrorists increases, so should the number of cyberattacks by terrorist groups show a corresponding increase.

There has never been a greater need for joint government and private industry cooperation to meet what will likely be the next great threat to the security of our nation's infrastructure. Reaction on the part of cyberattack victims (in both government and private industry sectors) continues to vary widely to both published and unpublished attacks. Some companies have taken an extremely aggressive stance, even to the point of reversing DoS attacks and actually counterattacking the DoS originators.^{xv} On the opposite end of the spectrum, many companies merely attempt to close the door to the attack and quietly look for ways to defeat attacks in the future, giving as little publicity as possible to the attack and hoping the attacker will seek another victim in the future. Still other companies have opted for litigation and criminal action to stop the attacks, understanding that only by pursuing actions which inflict legal pain will attacks be stopped.

Recent technology has enabled government agencies to electronically search an attacking computer for evidence of the attack,^{xvi} and the potential is not limited to purely defensive methods. According to the *New York Times*, the U.S. Department of Defense has set up a Cyberwarfare Center which provides offensive cyberwarfare capabilities, including strategies designed to "infect enemy software, upset enemy logistics, and disable enemy air defense systems." One immediate usage for the Center's programmers during the war in Kosovo was to conduct "attacks on Serbian computer systems in an effort to change banking records and deplete Serbian assets."^{xvii}

A review of published data indicates no unified approach in the defense of cyberattacks today, whether they be from teenage computer hackers or from dedicated terrorist groups bent on destroying the United States. While recent changes in state and national criminal laws have closed some of the more obvious loopholes, the basic fact is that as a nation we have failed to recognize the enormous nature of the threat to our society. Law enforcement attempts to plug gaping holes in electronic fences have been repeatedly and effectively thwarted by those who consistently place privacy above security. The recent attacks on the Pentagon and Twin Trade Towers of the World Trade Center may soften the resistance to law enforcement and intelligence surveillance legislation which, if passed, may include cell phone, Internet and e-mail tracing, increased access to credit-card billing information; roving wiretaps linked to people instead of

telephones, tougher penalties for terrorist crimes; and new methods to follow financial transactions by suspected terrorist groups.

A recent analysis of past cyberattacks makes some ominous predictions for the near future as the U.S. engages in its war on terrorism:^{xviii}

1. Electronic information sites in the U.S. and allied countries will be exposed to increasing attempts at defacing for the purpose of spreading disinformation and propaganda.
2. DoS attacks will increase, as will the use of worms and viruses.
3. Unauthorized intrusions into U.S. systems and networks will result in critical infrastructure outages and corruption of vital data.

Until the threat is recognized as not random and isolated, not the pranks of a few talented but misguided individuals, but is rather the opening salvo of a massive and deadly serious assault against the very fabric of our technological culture, no effective steps will be taken to prevent and neutralize the threat. It may just be that until we experience an "Electronic Pearl Harbor," we will continue to approach the problem in a piecemeal and ineffective manner, always playing catch-up with the other side and always at least one step behind in the ongoing war against computer literate criminals and cyberterrorists.

Preparation for the Attack

If one assumes that a future cyberattack is likely in some form, what are the steps, if any, which may be taken to protect networked governmental, corporate or even home computer systems? First and foremost, learn from other's mistakes by undertaking the following specific steps:

- **Policy review**

Every government and virtually every business in the United States now has at least one computer system. If employees have access to computers and systems, a review should be immediately taken of the current practices and procedures to determine appropriate use of network resources.

- Who has access and to which systems?
- What is their level of access?
- Exactly what are employees able to do with their access?
- Are written policies in place?
- Are they enforced?

Policy reviews should address e-mail and Internet use as well as basic security practices. There are many sample policies available and numerous reputable companies in

existence that conduct security audits. Much of what they do is plain common sense, but is generally based upon known methods of intrusion. If your organization is contemplating the use of a physical/technology security service for a review of your procedures, insure that those who conduct the audit have ample experience in their fields – in other words, use the best people you can find. Once policies are written and/or upgraded, they should be implemented as part of normal training, and every employee should acknowledge the receipt of training by signature.

After review by appropriate legal counsel, consideration should be given to the use of an on-system warning screen advising the user that the system confers no privacy rights and is to be used by authorized personnel only for official government/company business. Users should be notified that the system is subject to being monitored for appropriate use (perhaps defining the term “appropriate use”). The warning should further advise that system resources are subject to being retained and reviewed by the government and may be furnished to others, including law enforcement agencies, at the discretion of the government. Finally, users should be notified that by using the system they understand and consent to the provisions of the warning.^{xix} If not placed in a warning screen, the above should be incorporated into the government policy and should be acknowledged by all employees having access to system resources.

- **Firewalls and Virus Checkers**

Computers and networks without operating firewalls and up-to-date virus protection are similar to open entrance doors in homes – they are invitations for criminals to enter, steal, and vandalize.

Firewalls are generally considered necessary when using “always on” connections like T1 lines, cable and DSL connections because a typical telephone modem for a home line uses a different computer address (URL) each time the server is dialed. To test a particular computer’s vulnerability to outside probes, run the tests at Gibson Research (<https://grc.com/x/ne.dll?bh0bkyd2>), or at the Symantec site, (<http://www.symantec.com/securitycheck/>). These will show the need for firewall protection or will show how much protection an existing firewall offers.

One additional bonus for firewalls that should not be overlooked is the filtering capacity that they offer. Most provide filtering options ranging from no filtering to totally paranoid, and site-blocking features prevent most (but not all) unauthorized site visits. E-mail programs provide the same provision for blocking unwanted e-mail, but their ability to filter is somewhat limited.

Virus checkers are relatively cheap and offer substantial protection from e-mail and Web viruses, but must be frequently updated to be effective. The once laborious process of updating has been simplified and now is easily accomplished through automatic updates or one-button clicks.

Most virus protection software is based on pattern recognition of known virus characteristics. Since these recognition patterns are developed only after new viruses are identified, they are unable to prevent new and unrecognized viruses. Because no virus checking software offers 100 percent protection, an examination of company computer operating policies should be mandatory with a goal of limiting Internet access to only those employees who have a need for Internet use in their jobs.

E-mail use also should be examined and policies formulated to restrict the receipt of attachments, which often contain viruses. Thought should be given to notifying employees that their e-mail usage is subject to being monitored (they should sign a statement of acknowledgement) and then periodically examine e-mail content for inappropriate or excessive usage. Finally, a retention period for e-mail messages should be established to decrease storage requirements and incidental exposure. This period should be more than 30 days but less than a year. The ability to retrieve e-mail messages may become extremely important in the event that a cyberattack or virus renders the system inoperable.

- **Password Protection**

Individuals generally resist having to bother with passwords and when forced to do so, they often pick common words that are easily determined by scanning computers. To be safe, passwords should be a combination of letters and numbers and should be changed often. It is also a mistake to leave passwords in easily accessible places, such as under mouse pads or taped to the back of computers.

- **Security Patch Updates**

Many attacks could be thwarted simply by installing system patches provided by software manufacturers to plug known security breaches. Network administrators and individuals should check system vendor sites often for upgrades designed to repair system deficiencies.

Along the same lines, administrators should frequently check the FBI's National Infrastructure Protection Center (<http://www.nipc.gov/>) site and Carnegie Mellon University's CERT Coordination Center site, a federally funded research site located at (<http://www.cert.org/>) for updated cyberattack information. The CERT site is particularly helpful for home computer users as it offers practical tips in non-technical language.

The National Infrastructure Protection Center (NIPC) also provides a forum (InfraGard) which encourages the exchange of information between the U.S. Government and private sector members. NIPC acts as a facilitator to its members through the dissemination and exchange of information about infrastructure protection. InfraGard may be accessed through the NIPC site above or directly through <http://www.infragard.net>.

Data Backup

One of most common complaints among computer users involves system crashes, whether they are caused by a virus, sabotage, or malfunction. Other than virus protection, the easiest and cheapest way to protect a system is through periodic data backups. Most home users and small businesses, however, seldom backup their data on a frequently scheduled basis, and when the crash comes, which it inevitably does, weeks or months of work can be lost. Nor is it enough to simply copy the data. Provisions should be made to store the data at a secure off-site location for fire and theft protection.

Backup procedures and schedules should be thoroughly covered in the governmental policy or procedure manual. In addition to electronic data backup, vital hard copy files should also be archived for the unlikely event that extended power or computer outages might occur. Protection against transient power outages should be provided by UPS battery backup systems to eliminate unnecessary down time, with thought given to implementing generator-supplied power supply for the entire computer system.

- **Internal Security**

Finally, because most of the computer attacks today, including vandalism and theft, still originate from within organizations, internal security must be given more consideration. Information technology training, security education, and employee screening are all tools used to safeguard against internal attacks and theft. Periodic security audits from trusted outside agencies (discussed above), offer an unbiased view of the level of protection offered, as well as providing notice to company employees that infractions will likely be discovered and appropriate sanctions imposed.

While preventing all cyberattacks is impossible, with some basic planning and security awareness in mind, there are definite steps that companies, agencies and individuals can take to prepare their systems and personnel for the challenge. Failing to take these basic steps outlined above is akin to playing Russian roulette. Disaster may not strike immediately, but statistically it is bound to occur. What will you (or your organization) do when it does?

Conclusion

Many, if not most, governmental entities are on tightly restricted computer system budgets. Systems are expensive to purchase and maintain, especially with such a limited effective lifespan. If corners are to be cut, it is often in the systems security and training areas.

In light of the current threats, policy makers should carefully reconsider this view by asking one simple question: Just how much damage could be inflicted on my organization in a worst-case scenario attack on our computer system(s)? If a realistic initial appraisal determines a high level of vulnerability for continued operation, serious consideration should be given toward an immediate and thorough review of the

organization's information technology security. This security review can be implemented using the bullet point topics in the preceding section as guideposts. The review should begin with a policy review, and after inspection and corrective action on the other items have been completed, the policy should again be examined to insure all necessary changes have been incorporated.

It is not enough to make system and policy changes, however. All personnel (not just systems personnel) must be given adequate training in physical security, threat analysis, and emergency operations to insure that they understand likely threats and know what actions (including reporting procedures) to take in the event of a threat. In addition, computer systems personnel should be continuously trained in protection methods as outlined above and should be encouraged to be alert for potential violations and security breaches. The key to this training is to realistically portray the threat so that each employee understands his/her role in protecting both employees and the organization.

All personnel must understand that the likelihood of serious security breaches is now at such an increased level that their continued employment and possibly their physical safety depend upon compliance with organizational policy and threat consciousness. Security infractions and breaches must be thoroughly investigated and corrective action immediately taken, to include after-action reviews so that violations are not repeated. Employees should be encouraged to report violations, and inadvertent breaches should not be punished if reported. The idea is to prevent mistakes or violations from being buried through fear of reprisal rather than being reported and corrected.

Not all of the above suggestions are expensive. Many can be accomplished "in house," and with a minimum of effort. All systems should be reviewed immediately, however, as we are faced with dangers never before seen. President Bush advised following the September 11 attacks that we would most likely be engaged in a long war against very determined terrorists. Based upon the available evidence, those who have proclaimed themselves to be our enemies are well prepared. Are we?

Endnotes

- ⁱ "U.S.: First cyberattack by terrorists," *Reuters Report*, 5/5/98, <<http://news.cnet.com/news/0-1005-200-328992.html?st.ne.fd.mdh>> (4/25/00).
- ⁱⁱ "China Sect Claims Sites Under Attack," *Associated Press*, 7/31/99, <<http://www.jsonline.com/bym/tech/ap/jul99/ap-sect-hacking073199.asp>> (4/25/00).
- ⁱⁱⁱ David Noack, "Love Bug' Damage Worldwide: \$10 Billion," *ABP News*, 5/8/00, [Http://www.apbnews.com/newscenter/internetcrime/2000/05/08/lovebug_impact0508_01.html?s=syn.emil_1ovebug_impact0508](http://www.apbnews.com/newscenter/internetcrime/2000/05/08/lovebug_impact0508_01.html?s=syn.emil_1ovebug_impact0508)> (5/9/00).
- ^{iv} Andrew Quinn, "Risky Business; Computer Security a Top Issue," *ABC News*, 3/22/00, <<http://www.abcnews.go.com/sections/tech/DailyNews/survey000322.html>> (3/25/00).
- ^v Miguel Llanos, "Eco-extremists using e-mail bombs," *MSNBC*, 10/24/98, <<http://www.freerepublic.com/forum/a363216430d16.htm>> (11/2/98).
- ^{vi} Michael Kirkland, "NSC: 'Zombies' could cripple 'Net,'" *UPI Report*, 12/28/00, <<http://www.vny.com/cf/News/upidetail.cfm?QID=147841>> (12/29/2000).

- ^{vii} John J. Fialka, *War by Other Means*, (New York: W.W. Norton, 1997), pp. 104-105.
- ^{viii} Douglas Pasternak and Bruce B. Auster, "Terrorism at the touch of a keyboard," *US News and World Report*, 7/13/98, p.37, <<http://www.usnews.com/usnews/issue/980713/13cybe.htm>> (4/27/00).
- ^{ix} Ibid.
- ^x Sue Pleming, "Freeh: Cyber attacks doubled in '99," *Reuters*, 3/28/00 <<http://biz.yahoo.com/rf/000328/8y.html>> (4/1/00).
- ^{xi} Douglas Pasternak and Bruce B. Auster, "Terrorism at the touch of a keyboard," *US News and World Report*, 7/13/98, p.37. <<http://www.usnews.com/usnews/issue/980713/13cybe.htm>> (4/27/00).
- ^{xii} Simson Garfinkel, *Database Nation*, (Sebastopol, California: O'Reilly & Associates, 2000), p. 224.
- ^{xiii} Jim Krane, "Terror's 'Dark Undercurrent' Rises in America," *APB News*, 4/19/00, <http://www.apbnews.com/newscenter/breakingnews/2000/04/19/terror0419_01.html> (4/20/00).
- ^{xiv} Richard S. Groover, "Overcoming Obstacles: Preparing For Computer-related Crime," *FBI Law Enforcement Bulletin*, August, 1996, <<http://www.fbi.gov/library/leb/1996/aug962.txt>> (4/26/00).
- ^{xv} "Can you hack back?" *CNN News*, 6/1/00, <<http://www.cnn.com/2000/TECH/computing/06/01/hack.back.idg/index.html>> (6/3/00).
- ^{xvi} Patrick Riley, "Feds Use Convicted Pedophile To Create Internet Spy Software," *Fox News*, 8/16/00, <http://www.foxnews.com/national/081500/pedophile_riley.sml> (8/17/00).
- ^{xvii} Elizabeth Becker, "Pentagon Sets Up New Center for Waging Cyberwarfare," *New York Times*, 10/08/99, p. A16.
- ^{xviii} Michael A. Vatis, "Cyber Attacks During the War on Terrorism," *Institute for Security Technology Studies at Dartmouth college*, 9/22/01, <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf> 10/1/01.
- ^{xix} William C. Boni and Gerald L. Kovacich, *I-Way Robbery, Crime on the Internet*, (Boston:Butterworth-Heinemann, 1999), p. 166.

About the Author

Robert Thetford is a practicing attorney, and consults for police agencies and private industry. In 1998, he co-founded the Institute for Criminal Justice Education, Inc., a non-profit organization of which he is the managing director. He serves as an adjunct professor of criminal justice at Faulkner University, and teaches a variety of legal courses, including terrorism and web-based investigations.

* * * * *