# Emergency Response to Terrorism

## Objectives

At the end of this lesson, the student should be able to:

1. Understand the different types of terrorist organizations.
2. Discuss the different weapons used by terrorists.
3. Describe the factors that indicate a terrorist incident.
4. Discuss the five common steps of the Incident Command System (ICS) and the seven steps of the GEDAPER process.

## Case Study

A local shopping mall sounds a fire alarm, and both fire and ambulance are dispatched to the scene. Within minutes of receiving the alarm, dispatch is inundated with calls from the same location. The calls include reports of smoke, fire, and an explosion. The incident commander (IC) who is en route to the incident immediately asks dispatch to send additional units to the scene and to notify law enforcement. The mall is hosting a fashion show sponsored by a large cosmetics company. The cosmetics company had been criticized in the recent press regarding allegations of testing products on animals. The IC has increasing concerns about public safety, as an act of terrorism is possible.

You are the lead paramedic in the ambulance. Upon arrival at the scene, you can see visible smoke coming from one of the entrances to the mall. There are dozens of civilians running from the scene, making access to the mall parking lot difficult. Mall security directs you to an alternate entry point that has been cleared for first responders. The IC instructs your ambulance to stage in the mall parking lot away from the building.

Rapid access fire crews don their SCBAs (self-contained breathing apparatus) and enter the building. Within a few minutes, they exit the building and report their findings to the IC. The crew says they located the source of the smoke which is an exploded IED (improvised explosive device). They could only see one casualty, an adult male, who was clearly deceased as a result of injuries from the blast. The crew further reports that the victim was carrying a bag that appeared to contain several more "bombs."

The IC immediately orders units to withdraw from the vicinity of the victim and to assist with the evacuation of the mall. Law enforcement has arrived on the scene, and an ICS (incident command system), which facilitates the efficient interaction of different agencies is put into place.

As the lead paramedic, you are tasked with implementing triage. The triage area is cordoned off. Law enforcement searches all people entering and exiting the triage area. Everyone is well aware of the possibility of a secondary attack on the first responders. The majority of the injuries are from people who have hurt themselves during the rush to exit the building. One security guard is brought to the triage area with a penetration wound to the right thigh. The origin of the injury is suspected to be from shrapnel from the IED. A tourniquet has been used to treat the wound. A few elderly people are exhibiting signs of respiratory and cardiac distress as a result of the stress and anxiety of the incident. All the injured are quickly treated and transported to various hospitals.

Law enforcement sends the bomb technicians into the building to determine the nature of the explosion and to neutralize any additional threats. At the same time, law enforcement uses dogs to search the area in which the responding units have been staged for secondary devices. The bomb technicians confirm the initial findings of the rapid access crew. It appears that the victim was killed when trying to place a crudely constructed pipe bomb. The victim's bag contained three more IEDs. The bomb technicians manage to neutralize all three of the IEDs safely. After a few hours, the incident is completely resolved, and the mall is back in operation the next day.

## Introduction

It has often been quoted that freedom requires constant vigilance. The EMS profession also requires continued dedication and vigilance. In current times, terrorism is having an increasing impact on our daily lives. First responders now need to have an even broader base of knowledge and skills than ever before to deal with this growing threat. This expanded base of knowledge includes how to identify possible acts of terrorism and how to respond accordingly.

The Federal Bureau of Investigation (FBI) definition of terrorism is "the unlawful use of force against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in the furtherance of political or social objectives."[1]

The initial response by the provider to a terrorist incident may be no different than a routine EMS incident. Terrorism is a crime, and the provider needs to ensure that evidence is correctly preserved and that the scene remains undisturbed (with respect to life safety). Providers need to be able to deliver medical care safely to patients under the threat of terrorism, without the provider having to take unnecessary risks. The greater the understanding the provider has regarding terrorism, the better chance he or she will have in mitigating the risks.

According to the FBI, the US (including Puerto Rico) experienced 318 terrorist incidents from 1980 to 2005.[2] Although large-scale terrorist attacks have not occurred in the US since the 9/11 attacks, there have been several smaller occurrences of terrorism. Such incidents include mostly attacks by one or two people on various targets such as military facilities.

This article will discuss the many different types of terrorist organizations and the weapons that they might use. A potential terrorist attack will elicit a broad and complex response from many different agencies. As a medical provider, you will need to know how to fit into this complex response as well as how to ensure your safety and the safety of others.

## Types of Terrorist Organizations

The FBI broadly defines terrorism as either international terrorism or domestic terrorism. International terrorism occurs when a non-US person commits an act of terrorism against the US or other governments. In the context of this article, domestic terrorism is when US citizens plot or carry out a terrorist attack against the US.[4]

Some of the most infamous acts of international terrorism against the US were the 9/11 attacks which resulted in the deaths of thousands of people, including hundreds of first responders. International terrorism is further subcategorized as non-state supported terrorism, state-sponsored terrorism, and state-directed terrorism. Non-state supported terrorism is conducted by individuals without support or guidance from any government. State-sponsored terrorism are acts of terror that are directly financed or directed by a government. In state-sponsored terrorism, the government usually only instigates the act of terror, whereas the actual terror act is perpetrated independently by a terrorist group. Lastly, state-directed terrorism occurs when a foreign government conducts acts of terror directly against another country.[5]

EMS providers will most likely encounter acts of small-scale domestic terrorism. Examples of domestic terrorism that have occurred in recent times include the 2006 Sears Tower Plot, the 2007 Fort Dix plot in New Jersey, the 2008 bombing of the Times Square Armed Forces recruiting office, the 2009 Fort Hood shooting in Texas, and the 2009 New York subway plot.[6]

Most terrorist groups fall into the categories of violent religious groups (or doomsday cults), extremist socio-political groups, cyber terrorists, single-issue terrorist groups, and narco-terrorists. Violent religious groups frequently use mass murder as the endpoint of their cause. People who are not part of the violent religious group can be seen as targets to be eradicated due to their non-beliefs.[7]

Extremist socio-political groups are those who seek freedom from the current political, economic, or social norms of the country they reside in. These groups might also want to eradicate anything that threatens their current way of life such as foreigners or migrants with views that are different than their own. These groups often use terror tactics to further their cause.[8]

Cyber terrorists use technology as their weapon of choice. Cyber terrorists attempt to further their cause by illegally attacking the technological infrastructure of a target country. This technical infrastructure includes the Internet, power grid, government and corporate intranets, as well as telecommunications. The cyber terrorist will use a variety of techniques, such as hacking or viruses, to disrupt services, access private or confidential information, or misappropriate financial resources. Cyber terrorists are difficult to locate and can launch their attacks against the US from anywhere in the world.[9]

Single-issue terrorist groups are those groups who threaten and make use of violence to achieve their objective and spread their beliefs. Single-issue terrorist groups have causes such as anti-abortion, animal rights, anarchy, and racism. This type of group often starts out as a group that promotes its cause through peaceful and legal means, but as objectives are not reached, members of the group begin to take more extreme and violent measures to make their cause known.[10]

Narco-terrorists use terror tactics to take control of a region to allow them to produce illegal drugs without consequence. Narco-terrorists are usually well funded, trained, and armed. They have the ability to attack police, military, and government officials. Although other groups also support their cause with drugs, they do not manufacture or distribute the drugs and are therefore not narco-terrorists.[11]

In addition to the categories listed above, subcategories of terrorist groups include hate groups, patriot groups, militia groups, common-law groups, cult groups, single-issue groups, and lone wolves.[12] Hate groups target single issues such as abortion, homosexuality, or issues of race. The Ku Klux Klan is an example of a hate group. Patriot groups typically oppose the government and often overlap with hate groups. Militia groups are opposed to a federal government, and their goal is to have their state secede from the union. Common-law groups (also known as freemen) feel they have the right to interpret laws themselves and not be subject to rules of government. Cult groups that are not as violent as doomsday groups fall into this category and have a wide spread of different beliefs. Single-issue groups are often splinter-groups of non-terrorist organizations (and hence different to single-issue terrorist groups). These single-issue groups take matters into their hands to further their cause and commit an act of terror. Lone wolves are individuals who work alone and commit acts of terror in support of whatever cause they may have.[13]

Al Qaeda is a notorious international terrorist group in the Middle East. This group has divided itself into many different branches and often conducts synchronized, terror attacks with an ever-increasing level of complexity. Terrorism often finds a foothold in impoverished countries with weak or non-existent governments. Terrorists may also choose remote wilderness locations to set up training facilities that can be easily defended using guerilla tactics. Terror groups use recruiters to bring together the required personnel for an operation, as well as arrange the money and resources needed to orchestrate a terror attack. For example, the 9/11 attacks used 20 terrorists and dozens of other people to organize these events.[14]

Urban EMS providers will not likely come across terror organizations of this magnitude, but an understanding of how such groups function is important to gain an understanding of what makes up these organizations.

With a broad understanding of the different types of terrorist groups, it is crucial for the provider to understand that there are many peaceful and legal organizations. Not every organization or individual with a cause is a terrorist. The main differentiator for a terrorist group is that it commits illegal acts and often uses violence to achieve its goals. Terrorist groups may also join, or use different types of terrorism, to further their cause.

## Terrorist Weapons

When it comes to terrorist weapons one usually thinks of weapons of mass destruction (WMD) such as nuclear bombs and genetically-engineered viruses that lay waste to entire cities. Regarding domestic terrorism, a provider is more likely to encounter more conventional weapons such as firearms and explosives. According to the FBI, approximately two-thirds of terrorist attacks from 1980 to 2005 involved bombings.[15]

Typically, terrorist activities can be classed into five different categories: biological, nuclear, incendiary, chemical, and explosive (remembered by the acronym B-NICE). Another acronym that is favored by law enforcement is CBRNE which stands for chemical, biological, radiological, and explosive. Shootings are becoming a primary tool of terrorism but are not covered in either of these acronyms. Shootings may be dealt with using active shooter and mass casualty incident protocols in many jurisdictions.[17]

Biological agents are naturally or laboratory grown organisms that cause illness and death. Some biological agents can be weaponized to allow for dispersion across large areas affecting hundreds if not thousands of people. One of the main issues with biological agents when used on a large scale is that their initial dispersion may go completely undetected. The first indications of a biological attack may seem like a simple flu epidemic.

The Centers for Disease Control (CDC) classes the most dangerous biological agents as Category A agents.[18] Category A agents include anthrax, botulism, plague, smallpox, tularemia, and viral hemorrhagic fevers. These agents are considered to be particularly dangerous because they are easily dispersed, are easily transmitted from one person to another, have a high mortality rate and effect on public health, cause fear and panic, and require specialist intervention such as vaccination to prevent them from spreading.[19]

Category B agents are a lower threat and include cholera, glanders, Q fever, encephalitis, and ricin. Category B is considered to be moderately easy to distribute, causes mild illness, and has low mortality, but requires specialized diagnostics and surveillance.[20]

Category C agents are emerging diseases that can be readily weaponized due to their general availability (such as an epidemic in a developing country) and morbidity or mortality.[21]

The four common types of biological agents (including those in Category A) include viruses, bacteria, rickettsia, and toxins. Viruses require a living host to be able to exist and reproduce. Once a virus infects a person, the virus will replicate itself in healthy cells, and the disease will run its course. Viruses spread from host to host by vectors such as droplets, fleas, rats, saliva, and so on. Some viruses are more dangerous than others. The biggest problem with a virus is that the only cure is an antiviral agent, and these are not always available.

Certain types of deadly viruses include smallpox and viral hemorrhagic fevers. Smallpox has plagued humanity for over 12,000 years and has resulted in the destruction of more than one civilization, including the Aztecs and Incas of South America many centuries ago. In 18th century Europe, smallpox killed 400,000 people a year and was named the "speckled monster." With the invention of the smallpox vaccine, the disease was slowly eradicated. In 1977, the last natural case of smallpox was treated.[22]

Today smallpox only exists in tightly controlled laboratories in the US and the Russian Federation.[23] Smallpox is highly contagious and is spread using an aerosolized form of the disease.[24,25] Smallpox has a mortality rate of 10 to 30 percent.[26] The primary concern with smallpox is that vaccination is the only way to guarantee protection against the disease.[27]

Hemorrhagic viruses cause widespread bleeding throughout the body. The disease usually starts with flu-like symptoms that progress into internal and external bleeding. Hemorrhagic virus outbreaks are known to occur in Africa and South America, but outbreaks in the US are rare. Numerous factors must be taken into account to determine the mortality of the viruses (such as age, health, type of virus, and available healthcare), but a death rate of five to 90 percent can occur.[28]

Bacteria are different to viruses in that they don't need a host to multiply. Bacteria are self-sufficient, complex, and living organisms that can be up to 100 times bigger than a virus. Bacterial infections are combatted with antibiotics. The onset of bacterial infections presents with flu-like symptoms, which is not that different to the start of a viral infection. Examples of bacteria that are classed as Category A agent are anthrax, bubonic and pneumonic plague, and tularemia.[29,30]

Anthrax is a bacterium that initially stays dormant inside a protective covering called a spore. Anthrax is often associated with handling contaminated products of cattle, sheep, and horses.[31] Anthrax can infect the skin, gastrointestinal tract, or lungs. The lungs provide an optimal level of heat and moisture for the bacteria to be released from the spore, and as a result lung infections from anthrax are the most lethal. If not treated quickly, an anthrax infection of the lungs has a 90 percent mortality rate.[32]

The plague has ravaged humankind over the centuries causing tens of millions of deaths. The plague exists in two forms: bubonic and pneumonic. Infected rodents and fleas carry the bubonic plague. A flea will transmit the disease through its bite, and a rodent will spread the disease through contact with the rodent or its feces. The lymphatic system is the target of infection, and the lymph nodes can grow to the size and shape of a tennis ball (these lumps are called buboes). The disease will spread to the rest of the body if treatment is not received. Death usually results from sepsis. Fortunately, the bubonic plague is not contagious and is therefore not a prime choice for terrorists.[33]

The pneumonic plague is caused via inhalation of the plague bacteria. The pneumonic plague has a greater mortality rate than the bubonic plague as it is contagious. The pneumonic plague is, therefore, a much more attractive choice for a terrorist attack. The mutual signs and symptoms of both types of plague include fever, headache, muscular tenderness and pain, and shortness of breath.[34]

Humans usually contract tularemia through bites from ticks, deer flies, contact with infected animal skin, drinking contaminated water, and inhaling aerosolized particles or agricultural dust. Signs and symptoms vary depending on the route of infection, but a fever of 40°C (104°F) is common across all forms of tularemia. Of the many different forms of tularemia, the one of greatest concern is pneumonic tularemia.[35]

Pneumonic tularemia is the most severe and is caused when a person inhales infected dust or aerosol particles. Pneumonic tularemia can also result when other forms of tularemia are left untreated, and the infection spreads to the lungs. Signs and symptoms include coughing, pain in the chest, and dyspnea.[36] Tularemia is treated with antibiotics.

Rickettsia fits in between viruses and bacteria and live inside host cells of mammals and arthropods (such as spiders). Rickettsia is a very broad collection of organisms. For rickettsia to be a real problem regarding weaponization, it needs to be spread in aerosol form.[37] Q fever is an example of a rickettsia that originates from cattle, sheep, and goats. Infection to humans is achieved when contaminated particles are inhaled. Human to human tr Rickettsia is treated promptly, the mortality rate is less than one percent.

Toxins are naturally occurring substances that can be particularly deadly to humans. The toxins of choice for biological agents are botulism, SEB (Staphylococcal enterotoxin B), ricin, and mycotoxin.[38] To date, toxins have not been successfully used as WMD.[39]

Botulism is a muscle-paralyzing disease produced by bacteria. Foodborne botulism is the easiest to adapt to terrorist use. If untreated, victims die from respiratory failure when the diaphragm is paralyzed. Botulism is not contagious. Botulism is distributed through aerosolization, food supply infection, or injection. A vaccine for botulism is available. Signs and symptoms develop over six hours to 10 days (most commonly 12 hours to three days). Treatment is largely

supportive with an emphasis on respiratory care.[40]

SEB is a toxin produced by the Staphylococcus aureus bacterium (staph). Staph is extremely common and found on the skin and in the noses of one-quarter of human and animal populations. If a person breathes in SEB, fever, cough, dyspnea, nausea, and vomiting can occur at small doses. If a large dose is inhaled, the consequences can be much more severe.[41]

Ricin is less deadly than botulism but is fatal if left untreated. Ricin is made from castor beans and can be stored as a powder, aerosol agent, pellets, or as a solution in water or weak acid. Ricin interferes with the body's ability to create proteins which leads to cell death. If inhaled, ingested, or injected, death will occur within 36 to 72 hours from hypotension or respiratory failure if left untreated.[42]

Mycotoxins are derived from readily accessible fungi and include a broad range of toxins. At high doses, some mycotoxins can cause liver injury or liver cancer. All mycotoxins can be used for bioterrorism.[43]

Nuclear or radioactive weapons will most likely be radiologic dispersal devices or dirty bombs. These devices are designed to injure and kill through the use of conventional explosives, as well as spreading harmful radioactive material. Radioactive material can be sourced from hospitals, educational facilities, industrial sites, and power plants. Radioactive material can also be stolen from radioactive material waste sites. Although most nuclear weapons are tightly guarded in secure facilities, as many as 80 small suitcase-size nuclear bombs have been missing from the Soviet Union since 1998.

Patients who are exposed to radiation do not become radioactive. However, a patient who is contaminated with radioactive waste needs to be decontaminated by trained hazardous material personnel. People can be exposed to radiation through three different means, namely radioactive exposure without contamination with radioactive material, external contamination of the skin by radioactive material (the radiation may not necessarily have entered the body), or internal contamination through inhalation, absorption or ingestion of contaminated material (the radiation has entered the body and will irradiate from within). Once irradiated, a person will begin to exhibit signs and symptoms of radiation sickness such as nausea, vomiting, and diarrhea. Treatment is mainly supportive.

Providers should take measures to protect themselves from radiation exposure. There is no personal protective equipment to completely protect a person against radiation; time, distance, and shielding are the best ways to protect oneself. The amount of time of exposure must be reduced to an absolute minimum, the further from the radioactive source the better, and placing as much shielding between the provider and the radioactive source will limit exposure. Shielding is any object that can stop the path of radiation. Depending on the type of radiation that needs to be stopped, shielding can be as thin as a piece of paper, or as thick as several inches of lead (in the field it is near impossible to determine which type of radiation you are being exposed to).[44]

There are potentially hundreds of different ways in which an incendiary device can be constructed. The main difference between incendiaries and explosives is that incendiaries are designed to start a fire, and explosives are designed to detonate and cause damage. Terrorists can use any combination of mechanical, chemical, or electrical devices to start a fire. Incendiary attacks can be as simple as a burning match dropped into a wastebasket full of paper, or as complex as the aircraft full of jet fuel that were used in the 9/11 attacks. Medical providers will need to be prepared to treat a variety of burn patients. Providers should treat all incendiary devices as they would an explosive device, and leave the handling of these to trained bomb technicians. Extinguishing large fires, such as those that require more than a single fire extinguisher, should be left to firefighters.

Chemical agents are manmade agents that are classed as nerve agents, blister agents, choking agents, blood agents, and irritating agents. The manufacture of chemical agents was perfected during World War I, World War II, and the Cold War. The US does not use chemical agents in warfare.[45] Chemical agents can exist as a solid, liquid, or gas. Some agents are volatile and evaporate quickly, whereas others can persist in a targeted area from 24 hours to several weeks. Chemical agents can pose either a vapor hazard or a contact hazard to humans. Vapor hazard chemicals are inhaled, and contact hazard chemicals will enter the body through the skin.[46,47]

Nerve agents are exceptionally deadly and capable of causing a significant number of deaths with a small quantity of agent. Nerve agents attack the nervous system, and death can result within minutes from respiratory arrest. Common nerve agents include chemicals in the class of organophosphates. Organophosphates block the neurotransmitter cholinesterase which primarily causes hyperstimulation and eventual failure of the body's organs. G agents were developed during the two world wars by German scientists. Examples of G agents include sarin, soman, tabun, and V agent. It only takes 1.7 g of sarin to kill half the people exposed to this nerve agent (assuming a 70 kg body weight). V agent is 100 times more deadly than sarin.[48]

Nerve agents are recognized using the DUMBELS acronym. DUMBELS stands for defecation, urination, miosis (pupil constriction), bradycardia/bronchorrhea (excessive mucus in the lungs), emesis, lacrimation, and salivation. If a large group of patients presents with these signs and symptoms, nerve agent antidote such as DuoDote or MARK 1 nerve

agent antidote kits can be used for treatment MARK 1 kits are less commonly used to treat nerve agents these days.[49] If the kits are not available, large doses of atropine, such as 2 to 4 mg,[50] and pralidoxime 1 to 2 g IV (intravenous) infusion over 30 to 60 minutes post atropine administration can be used.[51]

Vesicant (or blistering) agents mostly work through contact with the skin. Vesicants cause severe blistering that are similar to blisters one would receive from a thermal burn. If a vesicant vaporizes and is subsequently inhaled, it will cause blistering of the respiratory tract. Examples of vesicant agents include sulfur mustard, lewisite, and phosgene oxime. Signs of skin exposure to a vesicant agent include red burning skin, immediate pain on contact, big blisters, gray skin discoloration, swollen eyes (which will often be kept closed), and even permanent blindness.

Signs of pulmonary exposure to vesicant agents include hoarseness, stridor, uncontrollable coughing, coughing up blood, and severe respiratory difficulty. Vesicant agents can cause permanent changes to body tissues. There are no civilian antidotes for the vesicant agents discussed (only the military has an antidote for lewisite called British anti-lewisite). Treatment of victims exposed to vesicant agents includes decontamination and support of the airway and breathing. Also, treat patients for burns and transport accordingly.[52]

Metabolic agents (commonly cyanide) interfere with the body's ability to use oxygen at the cellular level. Cyanide is a gas that has no color and has a smell that is similar to almonds. Metabolic agents can kill within minutes. Cyanide is commonly used in industrial processes, such as mining and plastic manufacture, and is also a byproduct of burning certain plastics and textiles.

Cyanide occurs naturally in fruit pits in very small quantities. Small doses of cyanide will have the signs and symptoms of hypoxia such as dizziness, headache, nausea, and vomiting. High doses of cyanide may cause dyspnea, tachypnea, flushed skin, tachycardia, altered mental state, seizures, unconsciousness, apnea, and cardiac arrest. Treatment of victims exposed to cyanide includes decontamination and support of the airway and breathing.[53] There are antidotes for cyanide poisoning, namely amyl nitrite and hydroxocobalamin (Cyanokit). These antidotes are both routinely carried on emergency vehicles. Amyl nitrite is administered to adults by crushing one to two ampules and allowing the victim to inhale the fumes. This is repeated until the person is conscious.[54] Cyanokit is administered to adults at a dose of 5 g through an IV at 15 mL/min. The dose can be repeated once. Cyanokit should not be administered through the same IV line as other drugs.[55]

Pulmonary (or choking) agents mostly work on the respiratory tract. Once inhaled, these agents damage the tissue lining the lungs and cause pulmonary edema, and subsequently respiratory difficulty and even respiratory failure. Two common pulmonary agents are phosgene (not to be confused with phosgene oxime) and chlorine gas. Chlorine has a much quicker onset than phosgene. Signs and symptoms of exposure to pulmonary agents include shortness of breath, tight chest, hoarseness, stridor, and severe coughing. Some victims will experience a complete airway obstruction from the swelling and will die within minutes.[56]
There are hundreds of accidental exposures to pulmonary agents each year when people incorrectly mix household chemicals, or during routine fire calls where toxic gases can be released into the atmosphere. Treatment of victims exposed to pulmonary agents includes decontamination and support of the airway and breathing. Encourage the patient to stay still as activity can hasten the onset of symptoms. There are no antidotes to pulmonary agents.[57]

Irritating agents (also known as riot control agents) are usually designed to incapacitate and not kill. These agents cause sudden burning of the eyes and upper airways (and any area of the body that is moist). The symptoms do not progress past the initial pain, and pulmonary edema does not occur.[58] These agents can cause panic if used in a confined space, and providers should expect orthopedic injuries if a crowd is exposed to irritating agents. Irritating agents are readily available and commonly used by law enforcement. Victims can be decontaminated using clean running water. Treatment is supportive with a focus on airway and breathing.[59]

The last weapon in the B-NICE acronym is explosives. There must be thousands of different types of military, commercial, and even recreational explosives available. Explosives can also be easily made using common industrial chemicals such as certain fertilizers and diesel fuel. The provider should expect a wide variety of injuries from explosions including external injuries such as burns and soft tissue injuries, and internal injuries such as barotrauma and internal bleeding. Not all injuries from explosives will be immediately apparent. In the event of an explosive attack, providers should be aware of the possibility of secondary explosions aimed at harming first responders. Additionally, explosions can be of sufficient force to significantly affect the structural integrity of a building. Providers should also be aware of the potential for building collapse.

## Terrorist Incident Indicators

The question as to how a provider can make the distinction between a terrorist and routine EMS incident is valid. In most cases, the provider will not know if it is a terrorist attack, as terrorists seldom announce their intentions before the attack takes place. Terrorists will also try to conceal the nature of the attack, possibly to dampen down the initial

response to the incident.

The best tool a provider can have is a high level of situational awareness. Being aware of suspicious activity or trends in calls or injuries may allow the relevant authorities to be more quickly notified as to the possibility of a terrorist attack. If a scene is a crime scene, the provider must coordinate carefully with law enforcement and should not interfere with the investigation. The provider should be aware of the hazards associated with a crime or terrorist scene and carefully make the decision as to whether he or she should delay entry until additional assistance arrives.

The Department of Homeland Security (DHS), has started the "If You See Something, Say Something™" campaign, which aims to raise public awareness about terrorism. The provider should be aware that he or she might be approached by people wishing to report suspicious activity, and should be able to direct the report promptly to the correct law enforcement agency. Suspicious activity is defined as any observed activity that could be related to terrorism. Suspicious activity includes many things such as unusual items or situations, strangers asking questions about secure facilities or operations, or someone monitoring a building or facility and taking notes in a peculiar way. It is important to understand that race, ethnic background, and religion do not constitute suspicious activity and need not be reported. Examples of suspicious activity would include an unattended bag in an airport or someone climbing the wall of a medical laboratory.[60]

Performing a threat analysis and pre-plan for terrorist attacks in a jurisdiction is similar in nature to performing these for non-terrorist incidents. If a pre-plan, for example, identifies an industrial facility that produces organophosphates, and determines that this facility is at a high risk for fire, then it could well be a target for terrorist activity. Terrorists could potentially attack the facility to cause damage to the surrounding areas or target the facility to steal dangerous goods.

When adding terrorist threats to a pre-plan or threat assessment, it is best to involve law enforcement officials who are experts in terrorist threat analysis. The threat analysis begins with determining if any groups may pose a terrorist risk. These groups were discussed in detail in the objective "Types of Terrorist Organizations."

Once the groups have been identified, the next step is to determine if there are any targets in which these groups have an interest. The DHS standard facility assessment criteria list includes the visibility of the site, if the site is critical infrastructure, how accessible the site is, the amount of hazards stored on site, and how many people occupy the site. Examples of sites that meet these criteria include military bases, government installations, high-profile or sensitive industries (such as weapons manufacturing), financial institutions, critical infrastructure (such as telecommunications, power, and water), weapons and explosives storage, areas of mass public gathering (sports stadiums, theme parks, malls, and so on), and educational and medical facilities.[61]

The DHS National Terrorism Advisory System (NTAS) will alert providers of the potential for attacks on the US and its territories. NTAS will issue bulletins and alerts to keep people up to date. An NTAS bulletin is used to keep people aware of emerging terrorist trends but does not necessarily indicate a threat. The bulletin includes a summary, duration of the alert, details of the threat, the affected areas, and tips on how one can help the current situation.[62] An NTAS alert is issued when there is a specific and credible threat to the US. The alert will include details of the threat, the region concerned, transport mode of the threat, targeted critical infrastructure, and actions that can be taken to limit the extent of the threat.[63] Alerts can be elevated or imminent. Elevated alerts warn that a credible terrorist threat exists. Imminent alerts warn of a credible, specific, and looming terrorist threat.[64]

The NTAS is not specifically issued to EMS but is broadcast via a variety of news, media, and other channels. Local protocol should determine how the NTAS bulletins and alerts are received and dealt with. Knowledge of NTAS alerts should be used to supplement the information in the local jurisdictions' own threat analysis. When responding to an incident, details of the incident should be compared to NTAS alerts to determine the likelihood of a terrorist incident. Information about the incident such as the location type, incident type, number of people, and witness statements might all be used to declare an incident a terrorist attack. For example, if you are dispatched to a church gathering where witnesses have reported hearing a loud bang and seeing smoke, and that there are lots of casualties – all of these point to the likelihood of a terrorist attack.

The B-NICE acronym that was discussed in the objective "Terrorist Weapons" is used to sum up the various weapons used by terrorists. A terrorist may choose to use a facility itself, such as a gasoline storage tank, as a weapon. The terrorist could then conceivably use a much smaller explosive device to try and trigger a much larger explosion and cause even more damage.

Categories such as the nuclear category require specialized equipment and handling to determine the extent of the damage and to prevent radiation from spreading. Local services may not have the ability to manage all categories of B-NICE, and should have in place a system to call in the experts when needed. Further, providers should be able to tell when they need to leave a scene if it is too hazardous. For example, consider the three aspects of time, distance, and shielding when dealing with nuclear incidents.

Providers should have a basic knowledge of hazardous materials, and every emergency vehicle should have a copy of the Department of Transportation's Emergency Response Guidebook (ERG). The ERG gives guidance on hazardous substances, as well as details on how to read the various hazardous material placards. It is important to be able to quickly identify if a hazardous material involved in an incident belongs to the biological, nuclear, incendiary, chemical, or explosive categories. If the materials involved in the incident do belong to one of these categories, and if any of the other indicators discussed in this objective are present, then an act of terror should be considered, and the appropriate agencies notified.[65,66]

Terrorists are adaptive. It is in their interest to continually seek out new ways to spread terror. Simply because B-NICE weapons and the use of firearms are the terrorists' current favorite choice, tomorrow might bring an entirely new weapon to your doorstep. Providers should continually stay up-to-date with the latest terrorist advances, and learn how those apply to the local jurisdiction.

## ICS and the GEDAPER Process

The National Incident Management System (NIMS) was developed to provide a template to assist with the management of major incidents that require the involvement of multiple agencies. NIMS is standardized in aspects such as terminology, classification of resources, training, certification, etc. NIMS is also designed to be non-restrictive and easily adapted to any situation. It is further designed to work for any agency, whether it be EMS, fire, law enforcement, military, and so on.[67]

The Incident Command System (ICS) is a sub-component of the command and management component of NIMS. ICS provides an incident concept with a modular organizational structure that is expanded as needed to suit incidents of any size. ICS optimizes resources to manage all aspects of the incident and to ensure optimal patient care. ICS provides a clear strategy to resolve an incident. ICS strives to eliminate duplication of effort and to control individuals or organizations from operating outside the ICS structure (often called freelancing).[68]

It is possible that an incident is so overwhelming that it seems impossible to decide on an approach. To combat making impulsive decisions, ICS offers five common steps that can be used in any incident. These common steps are: conducting scene size-up, evaluating the situation, setting incident priorities, estimating potential incident course and harm, and choosing strategic goals and tactical objectives.[69]

As a provider rolls onto a scene, he or she should already be gathering information about the scene and forming a general impression. If available, information from a pre-plan can prove to be valuable in doing a scene size-up. Other sources of information can include feedback from dispatch or other units already on scene. It is important to remember that scene size-up is not a once-off process that is done at the beginning of an incident. Scene size-up is a continuous process that needs to be as adaptive as the terrorist that is attacking.[70]

When evaluating the situation, the provider should look for physical signs, victim signs or symptoms, and weather patterns. Physical signs may give clues to what happened, such as smoke, fire, and blast damage. Victim signs and symptoms will give you a clue as to the types of injuries you may be dealing with. Scores of victims who are coughing or in respiratory distress may suggest a chemical attack, or victims with gunshot wounds may indicate an active shooter. Current weather conditions are of greatest significance when dealing with weapons that may be spread by the wind or affected by humidity such as poison gas, toxic smoke, or aerosolized biological agents.[71]

Once the initial scene size-up and evaluation are complete, the provider may be able to determine the type, cause, and status of the incident. The type of the incident will be one or more of the B-NICE categories. The incident cause is determined as being either accidental or intentional. Accidental cause would be something such as a motor vehicle collision involving a chemical tanker, and an intentional cause would be something such as terrorism. Lastly, the status of the incident will indicate if the incident is closed, ongoing but under control, or escalating and not under control.[72]

With a clearer picture of what the incident is about and its extent, incident priorities can be set. Safety is always the main priority, and the lives of first responders, members of the public, and victims must come first. Second to human life, essential infrastructure such as utilities (water, gas), transportation, and communication need to be protected. Finally, resolving the incident is also a priority. Good judgment should be exercised when setting the priorities. For example, if a terrorist is on an active shooting spree, it may be a priority to neutralize the terrorist before attempting to treat victims.[73]

Using all the information about the incident that has been gathered at this point and with a set of priorities available, providers should attempt to estimate the potential incident course and harm. Providers will try to predict if an incident will expand, and if so how much harm to people or damage to property will be caused. A typical scenario is at incidents involving explosive devices where terrorists may place secondary explosive devices to kill and injure first responders. Even if there are no secondary explosive devices, buildings may be damaged by explosions to the extent that they may collapse.[74]

The last of the five common steps is to choose strategic goals and set tactical objectives. Strategic goals are high level and generalized goals such as to prevent loss of life or minimize damage to critical infrastructure. Tactical objectives are more actionable and are implemented to achieve the strategic goals. For example, if a strategic goal is to reduce damage to critical infrastructure, tactical objectives such as to deploy additional fire crews to a facility and shut off fuel supplies to the infrastructure might be implemented to achieve that goal.

There are thousands of different hazardous materials, some more harmful than others. Given that hazardous materials are one of the weapons of choice of terrorists and that hazardous materials bring significant complexity to incidents, providers should have a basic understanding of the GEDAPER process. The GEDAPER process was developed by the National Fire Academy and is used for incident analysis. Once completed, the GEDAPER process will help providers resolve hazardous materials incidents safely and efficiently.[75]

GEPADER is an acronym for gathering information, estimating course and harm, determining strategic goals, assessing tactical options and resources, planning and implementing actions, evaluating, and reviewing. During the gathering of information step, the provider should safely attempt to obtain as much information as possible about the incident. Hazardous materials complicate this step in the sense that a provider should not risk exposing himself or herself unless he or she has adequate PPE and the training to use it. Providers should rather attempt to assess the scene from a safe distance. The ERG will be able to supply necessary instructions to the provider on how to handle the scene as well as supply additional information on the material concerned. Other sources of information include information received from dispatch, information from the scene size-up (the first common step in ICS), hazardous material warning signs or placards, information about weather conditions and topology that may affect the incident.[76]

The steps of estimating course and harm, determining strategic goals, and assessing tactical options and resources are similar to the respective common steps of ICS. The main difference is that each of these steps in the GEDAPER process is that they will be far more focused on the hazardous material itself, whereas the steps of ICS focus on all aspects of the incident. For each strategic goal, there must exist one or more tactical objectives to achieve the goal. For example, if a strategic goal is put in place to contain the spread of a hazardous material, then the tactical objectives such as cordoning off a hot zone (the area of contamination) and shutting off pumps supplying the chemical should be put in place.[77] Depending on the extent of a hazardous material incident, it is a possibility that the only course of action is to retreat to a safe distance, cordon off the area, and allow the incident to run its course.[78]

The planning and implementing actions step includes points that should be completed before an incident occurs. Standard operating procedures (SOPs) and standard operating guidelines (SOGs) are documents containing details about the functions, roles, and responsibilities for emergency personnel. Emergency services should also have conducted extensive training as well as simulation exercises on the SOPs or SOGs to ensure that any issues are worked out before an incident occurs. The Occupational Safety and Health Administration requires a site safety and health plan to be put in place for all incidents involving hazardous materials. This plan is a collection of checklists and details of how to manage the hazardous materials incident and how to ensure life safety. The SOPs, SOGs, and site safety and health will then be included with a written plan of action that lists all actions to be conducted by first responders to resolve an incident.[79]

The evaluating step is used to see if the current plan is achieving set goals and objectives. If plans are failing or goals are not being met, then changes should be implemented to adapt to the present circumstances. If a plan is not working, it should be modified. The review step is conducted as each strategic goal is achieved, or as needed throughout a prolonged incident. If the GEDAPER process has been properly implemented and executed, typically there should be no or minimal problems. If problems are discovered with the plan, they should be noted and analyzed, and changes should be made to the plan to prevent the same problems from reoccurring.[80]

## Case Study Conclusion

On the face of it, this incident could have been a simple fire in a shopping mall. Explosions frequently happen with fires and these are not always alarming to firefighters. As the IC received information about the incident while en route, something didn't seem right. There was too much going on at the mall for this to be a straightforward and routine fire call. The mall and cosmetics company might have been part of a briefing or pre-plan as a potential target. The IC decided to err on the side of caution and call for assistance.

Mall security, which seemed to be pretty organized, may also have participated in exercises with EMS, fire, and law enforcement. As the incident unfolded, everyone knew what they had to do, and things worked well. Everyone knew the risks associated with terrorism and were on the lookout for dangers such as secondary devices.

The question may be asked as to whether or not it was a good idea to send firefighters to the source of the explosion, but that sort of thing is the IC's call. Uncertainty still existed as to the nature of the explosion, and if it was not terrorist-related, such as a gas main, the firefighters would be better adept at handling it. The second the firefighters realized the explosion was as a result of an IED, they backed off and handed the incident over to the bomb

technicians.
After investigation of the incident, it turns out the deceased was a domestic terrorist acting as a lone wolf. The terrorist used to be part of an animal anti-cruelty organization but was fired due to a violent outburst and having extremist views.

## Conclusion

This article gave insight into the nature of terrorism and the types of weapons that can be used. Terror is insidious and can happen in any provider's jurisdiction without warning. Ensuring that one has the knowledge, training, and experience to differentiate between routine calls, crime scenes, and terrorist incidents is crucial to the successful outcome with an emergency response to terrorism.

Just as a provider has to stay current on topics such as basic cardiopulmonary resuscitation, advanced cardiac life support, and many other medical topics, so does the provider need to remain aware of topics such as the latest developments in terrorism.



References

1. Article. Introduction to the Emergency Response to Terrorism (IERT), March 2010. Federal Emergency Management Agency.
2. Internet. Federal Bureau of Investigation. Terrorism 2002-2005. https://www.fbi.gov/stats-services/publications/terrorism-2002-2005. Accessed: 06/28/2016
3. Graph created by CE Solutions Author. Statistics from Op cit. Terrorism 2002-2005.
4. Book. Nancy Caroline's Emergency Care in the Streets, 7th Edition. Andrew N. Pollak, MD, FAAOS. Page 2290
5. Ibid.
6. Ibid. Page 2291
7. Ibid.
8. Ibid.
9. Ibid. Page 2292
10. Ibid.
11. Ibid. Page 2293
12. Ibid.
13. Ibid.
14. Ibid.
15. Op cit. Terrorism 2002-2005
16. Graph created by CE Solutions Author. Statistics from Op cit. Terrorism 2002-2005.
17. Op cit. IERT. Module 1, Page 11
18. Ibid.
19. Ibid.
20. Internet. Department of Homeland Security. Biological Attack – Human Pathogens, Biotoxins, and Agricultural Threats. https://www.dhs.gov/xlibrary/assets/prep_biological_fact_sheet.pdf. Accessed: 07/11/2016
21. Internet. Centers for Disease Control and Prevention Classification of Bioterrorism Microorganisms. http://ocw.jhsph.edu/courses/BiologicalAgentsOfWaterAndFoodborneBioterrorism/PDFs/WaterFoodTerror3.pdf. Accessed: 07/11/2016
22. Op cit. Pollak. Page 2304
23. Op cit. IERT. Module 1. Page 12
24. Op cit. Pollak. Page 2305
25. Internet. US National Library of Medicine. Edward Jenner and the history of smallpox and vaccination. Stefan Riedel, MD, PhD. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1200696/. Accessed: 07/11/2016
26. Op cit. IERT. Module 1. Page 12
27. Ibid.
28. Op cit. Pollak. Page 2305
29. Ibid. Page 2306
30. Internet. Department of Homeland Security. Biological Attack – Human Pathogens, Biotoxins, and Agricultural Threats. https://www.dhs.gov/xlibrary/assets/prep_biological_fact_sheet.pdf. Accessed: 07/11/2016
31. Op cit. IERT. Module 1. Page 12
32. Op cit. Pollak. Page 2306
33. Ibid.
34. Ibid.
35. Internet. Centers for Disease Control and Prevention. Tularemia. https://www.cdc.gov/tularemia/signssymptoms/index.html. Accessed: 07/11/2016

36. Ibid.
37. Internet. Medscape. Rickettsial Infection. Mobeen H Rathore, MD, CPE, FAAP, FIDSA. http://reference.medscape.com/article/968385-overview. Accessed: 07/12/2016
38. Op cit. IERT. Module 1. Page 13
39. Op cit. Pollak. Page 2307
40. Internet. Centers for Disease Control. Facts about Botulism. http://emergency.cdc.gov/agent/botulism/factsheet.asp. Accessed: 07/12/2016
41. Internet. Centers for Disease Control. Staphylococcal Food Poisoning. http://www.cdc.gov/foodsafety/diseases/staphylococcal.html. Accessed: 07/12/2016
42. Internet. Centers for Disease Control. Facts about Ricin. http://emergency.cdc.gov/agent/ricin/facts.asp. Accessed: 07/12/2016
43. Internet. Centers for Disease Control. Toxins. https://www.cdc.gov/biomonitoring/toxins.html. Accessed: 07/12/2016
44. Op cit. Pollak. Page 2311
45. Ibid. Page 2298
46. Op cit. IERT. Module 1. Page 16
47. Op cit. Pollak. Page 2298
48. Ibid. Page 2301
49. Ibid. Page 2302
50. Ibid. Page 552
51. Ibid. Page 571
52. Ibid. Page 2299
53. Ibid.
54. Ibid. Page 550
55. Ibid. Page 561
56. Ibid. Page 2299
57. Ibid.
58. Internet. Chemical Hazards Emergency Medical Management. Chlorine – Prehospital Management. https://chemm.nlm.nih.gov/chlorine_prehospital_mmg.htm. Accessed: 07/15/2016
59. Op cit. IERT. Module 1. Page 16
60. Internet. Department of Homeland Security. If You See Something, Say Something. https://www.dhs.gov/see-something-say-something/. Accessed: 07/18/2016
61. Op cit. IERT. Module 2. Page 31
62. Internet. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/15_1214_ntas_sample_elevated_alert.pdf. Accessed: 07/13/2016
63. Internet. Department of Homeland Security. https://www.dhs.gov/topic/ntas. Accessed: 07/13/2016
64. Internet. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/NTAS_v2_poster_01.pdf. Accessed: 07/13/2016
65. Op cit. Pollak. Page 2260
66. Op cit. IERT. Module 2. Page 33
67. Op cit. Pollak. Page 2200
68. Ibid. Page 2200
69. Op cit. IERT. Module 4. Page 52
70. Ibid. Page 53
71. Ibid.
72. Ibid.
73. Ibid.
74. Ibid.
75. Ibid. Page 54
76. Ibid.
77. Ibid. Page 55
78. Ibid. Page 58
79. Ibid. Page 59
80. bid. Page 61