RELATED TERMS

- Site Safety
- Accountability
- Incident Site Management

Lessons Learned Information Sharing
www.LLIS.gov

BEST PRACTICE

PRIMARY DISCIPLINES

- Law Enforcement
- Fire
- Emergency Management

Incident Site Security: Secondary Attacks

PURPOSE

This Best Practice discusses procedures for preventing and mitigating the effects of secondary attacks at terrorist incident sites.

SUMMARY

Effective incident site security (ISS) requires immediate action to address the threat of secondary attacks. This Best Practice reviews key elements that secondary attack standard operating procedures (SOPs) should address: identifying/locating devices and/or potential attackers, disarming secondary devices, defining response logistics, establishing perimeter security, and validating threat.

DESCRIPTION

Secondary attacks follow an initial incident and generally target emergency responders and/or gathered bystanders at an incident scene. The most common form of secondary attack is a pre-planted, self-detonating explosive device located near an initial incident site. However, devices can utilize a number of designs and agents, including chemical, radiological, or biological releases. This document focuses on threats posed by pre-planted explosive devices.

Statistics suggest that secondary devices are present at half of all terrorist incident sites. Secondary attacks first garnered attention in the United States following several attacks in the Atlanta area in 1997. Seven people were seriously injured when a secondary explosive device hidden in a dumpster detonated 45 minutes after an attack on a family planning clinic. Two emergency responders were among the injured. A month later, law enforcement officials located and disarmed a secondary attack device at the scene of a nightclub bombing in downtown Atlanta.

Following the 1997 secondary attack on emergency responders, the Department of Justice released a training video entitled "Surviving a Secondary Device." The video details strategies for anticipating secondary devices, managing the scene, and protecting the public.

Use of secondary devices has become a disturbing trend, occurring numerous times in recent years. For example, emergency responders removed two secondary explosive devices from the incident scene and surrounding areas at the 1999 Columbine High School shootings in Littleton, CO. The 2002 bombing of a nightclub in Bali, Indonesia was characterized by a small initial explosion, which drove patrons into the street, followed by the secondary detonation of a massive truck-bomb. Similarly, the March 2004 train bombing in Madrid, Spain, included two unexploded secondary devices set to detonate one hour after the initial ten explosions on crowded commuter trains in the city center.

Developing Standard Operating Procedures: Evolving Threats, Evolving Procedures

Secondary dangers require that emergency responders simultaneously safeguard the public and protect themselves. The increased threat of secondary attacks has created a new array of dangers and challenges. Secondary attack SOPs *must* anticipate and address these new hazards. They must enable responders to locate and disarm secondary devices. Other ISS procedures must also consider the potential for secondary attacks and devices. Proceeding without executing such SOPs puts responders and the public at risk, and can ultimately hamper the response effort. This Best Practice reviews the key elements that must be addressed in secondary attack SOPs.

Identifying/Locating Threats for Secondary Attacks

The most common type of secondary attacks is a pre-planted, self-detonating explosive device. Secondary attack SOPs must be designed to locate such devices, if present, for removal and/or disarmament.

As soon as an incident is categorized as a suspected terrorist attack, the Incident Commander (IC) or another member of the Command Team should assign one person to be a "sweeper." The sweeper (also known as a "spotter") is responsible for visually scrutinizing the incident scene and surrounding areas for secondary devices and suspicious and/or unauthorized individuals. An individual familiar with the site may accompany sweepers to assist in identifying suspicious or out-of-place persons and/or objects. Video or digital photography may be of assistance in this process.

Other types of secondary attacks, including suicide bombers or chemical, biological, or radiological release, are all possible, although less common than pre-planted self-detonating devices. Prevention of these less common attacks is dependent on effective site security procedures—specifically, perimeter security procedures.

Sweeping should begin at the center of the incident scene and work outward in concentric circles. Locations of particular interest to sweepers include trashcans, book bags, suitcases, parked cars, and suspicious individuals, all of which offer ideal concealment for secondary devices. After the initial all-clear, responders should continue to be vigilant for suspicious objects and other potential secondary devices throughout the response.

The specifics for executing these procedures will vary across jurisdictions. Some jurisdictions, like Phoenix, AZ, require Bomb Squad personnel to conduct an incident site sweep at suspected terrorist scenes. Others, like Waterloo, IA, only require personnel with explosives experience in full structural personal protection equipment (PPE).

Disarming a Secondary Device

If emergency personnel locate a secondary device, the "hot" zone around the incident site should immediately expand to include 300 feet around the suspicious device. Because proximate cell phone or radio use may inadvertently detonate secondary explosive devices, use of this equipment should be prohibited within 500 feet of the suspected device. SOPs should dictate clearing the area and requesting immediate Bomb Squad assistance. No untrained or unprotected personnel should touch or move the suspected device. Normal operations may begin or resume after explosive experts have declared the device disarmed or destroyed and give an "all clear". Some jurisdictions have integrated robots into SOPs for disarming and/or removing secondary devices.

Jefferson County, Colorado, used robots to aid in secondary device removal at the scene of the Columbine shootings in 1999.

Defining Response Logistics

Terrorists often place secondary devices in locations where responders or victims are likely to gather. Response logistics must reflect this danger. Upon arrival, first-on-scene responders should avoid congregating in the same area unless otherwise instructed, to minimize responder-casualty potential in the event of an attack. As a response increases in scope, the support zone (or cold zone), where all staging, reception and other congregational activities occur, should also be thoroughly checked for secondary devices.

At the 1999 Columbine High School shootings, large secondary devices were discovered in the shooters' cars. The vehicles were located in the student parking lot where responders were preparing to place an engine company to support bomb disposal operations.

Similarly, placement of the incident command post (ICP) should be made with secondary attack dangers in mind. The ICP should be located approximately 300 yards from an incident scene in an area that has been thoroughly checked for secondary devices.

The collapse of World Trade Center (WTC) 2 destroyed the ICP. This event demonstrated how a secondary attack can undermine response efforts.

Inside the Hot Zone: HazMat Precautions

The incident site itself should be considered a "hot" zone, and treated as a highly hazardous area until the sweeper declares it clear of secondary devices. The number of personnel operating in the hot zone should be kept to an absolute minimum. Personnel retrieving and treating victims should employ "swoop and scoop" procedures, transporting victims out of the hot zone before triage and treatment. Similarly, fire personnel should employ "hit and run" fire suppression tactics, constantly moving in and out of the zone, until an expert has declared the hot zone free of secondary devices. For further protection, responders should shield themselves and victims with physical barriers. Emergency service vehicles such as fire trucks and ambulances can be used to erect a temporary barrier between victims and the hot zone. Trying to render normal patient care or fire fighting tactics can put responders and victims in mortal danger.

The Georgia Emergency Management Agency (GEMA) recommends utilizing engulfed-car SOPs for fire and emergency medical services personnel at suspected terrorist incident sites. These SOPs dictate full structural PPE including a self-contained breathing apparatus (SCBA) and the swift removal of victims before the administration of any treatment. Georgia's SOPs are described in the training video entitled, "Surviving a Secondary Device" and made by the Department of Justice, in cooperation with GEMA.

Establishing Perimeter Security

Effective perimeter security procedures are essential for preventing and mitigating the effects of secondary attacks. Entry and exit controls limit the number of people at the incident scene, allowing responders to search more easily for secondary devices and minimizing casualties in the event of a second attack. Similarly, preventing unauthorized individuals from entering the site limits the ability of terrorists to carry out a second attack in person.

The Georgia Emergency Management Agency uses the following adage as its guideline for outer perimeters: "If you can see what the bomb technicians are doing, you are too close."

Outer perimeters must be large enough to protect the public and emergency support functions in the "cold zone" from secondary attack dangers emanating from the incident site. The Federal Bureau of Investigation suggests using 1000 yards from the incident as

standard procedure. For more on outer perimeters, see the *Lessons Learned Information Sharing* Best Practice: "Incident Site Security: Outer Perimeters."

Validating Threat

Reliable secondary attack threat information is critical at incident sites. The Pentagon site experienced three full evacuations during the first hours of operations, only the first of which was based upon validated threat information. The other two evacuations, based on un-validated information, resulted in unnecessary physical and mental toll upon the responders. Planners should consider communications security and threat validation when developing secondary attack evacuation SOPs.

RESOURCES

Sample Procedures

Phoenix, AZ Fire Department. *Phoenix Regional Standard Operating Procedures: Hazardous Materials Weapons of Mass Destruction, Chemical, Biological, Radiological Response Operations*
http://phoenix.gov/FIRE/20414b.html

Pullman, WA Fire Department. *Response and Decontamination Procedures for Biological Agents.*
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=13466

Township of Shuniah, Ontario, Canada. *Sample Operating Guidelines: Fire Service Response to Accidental or Intentional Release of Nuclear, Biological or Chemical (NBC) Agents or Other Unknown Agent*.
http://www.shuniah.org/FireSops/Sample%20Operating%20Guideline.htm

Waterloo, IA Fire Rescue. *Responding to Terrorist Incidents: A Primer*.
http://www.wplwloo.lib.ia.us/wfr/terror.html

References

Arlington County, VA. *Arlington County Conference Report: Local Response to Terrorism: Lessons Learned from the 9-11 Attack on the Pentagon*. 01 Nov 2003.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=10355

Briese, Garry. "Terrorism and the Fire Service: Overview, Observations, and Trends," *Fire Chief*, vol. 42, iss. 11. Nov 1998.

Corbitt, Cathleen. *Explosions at a Fire Scene.* Interfire Online.
http://www.interfire.org/features/explosions_at_firescene.asp

Department of Homeland Security. *National Incident Management System*. 01 March 2004.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=7975

Federal Emergency Management Agency. *Summary of Post 9/11 Reports "Lessons Learned*." Oct 2002.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=157

Fuller, T.C. *Terrorism: A Law Enforcement Perspective.* Anti-Defamation League, Law Enforcement Agency Resource Network.
http://www.adl.org/learn/columns/Training_tips.asp

Gips, Michael A. "Secondary Devices a Primary Concern," *Security Management*, vol. 47, iss. 7. Jul 2003, p. 16.

Hicks & Associates. *Project Responder: National Technology Plan for Emergency Response to Catastrophic Terrorism.* Apr 2004.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=9809

International Association of Chiefs of Police. *Leading from the Front: Law Enforcement's Role in Combating and Preparing for Domestic Terrorism*. Oct 2001.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=6538

International Association of Fire Chiefs. *Performance Capability Recommendations: Second National Conference on Strengthening the Public Safety Response to Terrorism.* 2002.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=8486

Jackson, Brian A., D.J. Peterson, James T. Bartis, et al. *Protecting Emergency Responders: Lessons Learned from Terrorist Attacks.* RAND Science and Technology Policy Institute. 2002.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=7401

McKinsey and Company. *Improving NYPD Emergency Preparedness and Response.* 19 August 2002.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=159

McKinsey and Company. *Increasing FDNY's Preparedness.* 01 Aug 2002.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=379

Office for Domestic Preparedness. *Emergency Responder Guidelines.* 01 Aug 2002.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=136

Oklahoma Department of Civil Emergency Management. *After-Action Report: Alfred P. Murrah Federal Building Bombing 19 April 1995 in Oklahoma City, Oklahoma.* Nov 1995.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=6513

Titan Systems Corporation. *Arlington County After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon.* 30 May 2002.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=483

United States Fire Administration. *Wanton Violence at Columbine High School,* USFA-TR-128. Apr 1999.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=732

Winton, Richard. "SWAT *Team Robot Is Ready to Roll,*" *Los Angeles Times*. 28 May 2004.