Session No. 529

Protecting Critical Infrastructure and Personnel

Brian Bennett, CSP

Introduction

In today's new world order, a terrorist will be interested in causing harm to our communities using any means possible. It is critical that facility personnel are trained to recognize the sign of potential terrorist activity, and know how and to whom to report that information.

What is Terrorism?

Terrorism is derived from the Latin word terrere, which means to tremble. Terrorism is defined in the United States Code, Title 22, Section 2656(f) d, as "premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience.

Terrorist acts are intended to:

- Instill fear
- Coerce
- Intimidate
- Get people to change their day to day activities

in furtherance of social or political objectives.

The goals of terrorism include:

- Casualties/Fatalities
- Destruction of Critical Infrastructure
- Disruption of the Economy
- Change in daily routine

There are no characteristics common to all terrorists or terrorist attacks. However, there are activities that can be observed and reported to law enforcement personnel for investigation. There are eight indicators of possible terrorist activities:

1. Pre-operational surveillance: The terrorist may conduct surveillance of a target to gather information that would be useful in planning and executing an attack.
2. Seeking Information/Elicitation: A terrorist may attempt to gather useful information about a target by questioning personnel that are familiar with the asset being targeted.
3. Probing/Tests of Security: A terrorist may attempt to test the various security procedures of systems that are in place to protect an asset from attack.
4. Intrusion: Intrusion is different from probing in that the adversary has actually gained access into a restricted area for the purpose of collecting information or stealing something of value.
5. Acquiring Supplies: The adversary will attempt to collect the materials needed for the attack, such as weapons, uniforms, identification, vehicles, etc. These supplies may be acquired legally or illegally.
6. Suspicious people who do not belong: Suspicious people who do not belong or fit in a certain area or conducting suspicious activities may also be a potential indicator of terrorist activity. For example, a person may be observed photographing a government building in great detail from various angles.
7. Dry run/Trial run: The terrorist may attempt to conduct a trail run of their attack to test the details of their plan as well as the security systems and response from the asset.
8. Deploying assets/Getting into position: This is the final sign and it occurs immediately before the attack is perpetrated as the terrorist deploys personnel and equipment to the area they will be used as a weapon.

Any of these events may appear, by itself, unrelated to terrorist activity. Some in fact may be harmless with no criminal intent. Since it is very difficult for a lay person to ascertain the significance of what has been observed, it is best to report it to law enforcement.

What Are Critical Infrastructure and Key Assets

In order for terrorists to accomplish their goals, they must attack targets that will cause mass casualties, economic loss, destruction of property, or environmental damage. Potential targets that meet these criteria include:

- Critical infrastructure
- Areas with high density population
- Symbolic structures
- Government/military facilities
- Historical/cultural facilities
- Transportation systems
- Economic infrastructure

Critical Infrastructure is defined in the USA Patriot Act of 2001 as “the physical and cyber systems so vital that their incapacity or destruction would have a debilitating effect on national security, economic security, or public health and safety.” Simply translated, that means the personnel, physical assets, cyber, and communications systems we depend o each day to maintain our standard of living. In the United States, 85% of our critical infrastructure is owned by the private sector.

Key assets are defined as a specific component of a critical infrastructure. Key assets include:

- People

- Information
- Property

Types of Terrorist Attacks

A terrorist event can be executed by one of three methods:

1. An insider: an attack perpetrated by someone from within the organization, such as an employee.
2. An outsider: an attack perpetrated by someone external to the organization.
3. Collusion: an attack perpetrated by an outsider working in cooperation with someone from within the organization.

An asset may be attacked or exploited in one of four ways:

1. The asset may be the target: The asset itself may be the target of the attack, because there was something present that made the asset attractive as a target (such as large groups of people in a small area).
2. The asset may be collateral damage: An asset may be adversely impacted by virtue of its location. Collateral damage is unintended damage. For example, during the 9/11 attack in New York City, even though 7 World Trade Center was not targeted, it was destroyed due to collateral damage.
3. The asset may be used as a diversion: An asset may be attacked as a diversion from the primary attack. A terrorist may attack a target to draw resources away from the primary target, which may then be vulnerable.
4. The asset may be stolen, hijacked, or diverted: Some assets may be portable, and can be stolen, hijacked, or diverted and used as a weapon. An example would be a railcar containing a toxic chemical.

The terrorist can perpetrate any number of attacks, including:

- Cyber
- Economic
- Assassination
- Kidnapping
- Weapons of Mass Destruction (WMD)

This paper will focus on the type of attack that has the greatest potential to accomplish the terrorist's goals: an attack involving a weapon of mass destruction (WMD). There are five types of WMDs:

- Biological
- Nuclear
- Incendiary
- Chemical
- Explosive

Biological weapons are those that cause illness to exposed personnel. Biological weapons include bacteria (such as anthrax), viruses (such as small pox), or toxins (such as ricin).

Nuclear weapons are those that involve radiological agents. There are three main types of nuclear or radiological weapons:

1. Nuclear weapon involving the fission of fusion of atoms resulting in a nuclear explosion;
2. Radiological dispersal device, which is a conventional explosive which is used to disperse radioactive material over a wide area;
3. Intentional release of radiation, such as an attack against a nuclear power plant which results in the uncontrolled release of radiation.

Incendiary attacks are those that use fire as a weapon to cause death and/or destruction.

Chemical weapons can be broken down into five general categories:

1. Nerve agents, which are essentially pesticides for humans. These agents affect the central nervous system and cause death almost immediately if a sufficient dose of a properly formulated and dispersed agent is used. Examples of nerve agents include VX and Sarin.
2. Blister agents are chemicals that cause massive blistering of the external skin or internal systems (such as the respiratory or digestive systems) upon inhalation or ingestion. Once the blisters break, the victims often suffer shock from the massive loss of body fluids as well as increased risk of infection due to large, open wounds. Examples of blister agents include mustard gas and Lewisite.
3. Blood agents are those chemicals that interfere with the blood's ability to bind with oxygen, or impair the cells ability to extract the oxygen from the blood. Carbon monoxide is a common blood agent.
4. Choking agents are those chemicals that affect the respiratory system. Typically, choking agents are corrosive chemicals that cause burns and the resulting edema after inhalation. Victims die primarily from the constriction of the breathing passages from the burns, as well as edema. Examples of choking agents include chlorine and ammonia.
5. Incapacitating agents are those chemicals that are used to temporarily incapacitate a victim rather than kill or seriously injure them. Incapacitating agents include Mace and tear gas.

Explosive weapons are the most commonly used weapon by terrorists, being involved in more than 75% of all terrorist incidents.

Review of the CFAT Regulation

The U.S. Department of Homeland Security issued the Chemical Facility Anti-Terrorism Standards (CFAT), 6 CFR 1927, on April 9, 2007. The rules requires facilities that store or handle a listed chemical above a specified threshold to perform a screening process, a security vulnerability analysis, and implement a site specific security plan.

Key asset screening process

The purpose of a screening process is to determine the attractiveness of an asset as a target to a terrorist. Considerations used in the screening process include:

- potential for casualties
- economic impact

- destruction of critical infrastructure
- criticality of the asset
- effect on safety, health, or national security

Security vulnerability analysis

A security vulnerability analysis builds on the screening process. The vulnerability analysis looks at potential vulnerabilities that can be exploited by a terrorist in great detail. Typically, a security vulnerability analysis is approached from two viewpoints:

1. Asset based: Each key asset is reviewed to determine the effects if it were to be destroyed or degraded.
2. Scenario based: Likely attack scenarios are evaluated to identify vulnerabilities and develop corrective measures.

Security Plan

A site specific security plan is developed from the information obtained in the security vulnerability analysis. The security plan will outline the physical systems and polices and procedures that will be used to reduce the asset's vulnerabilities to an attack.

Conclusion

Counter-terrorism is everyone's responsibility. No asset or person is immune from attack. Terrorism by its very definition is random violence, and will impact anyone and everyone who happens to be in the wrong place at the wrong time. An educated, prepared, and aware population is the best weapon against terrorism.

Reference

Bennett, Brian Identifying, Understanding, and Assessing Terrorism: Protecting Critical Infrastructure and Personnel, John Wiley & Sons, 2007