CHAPTER 8

SECURITY REQUIREMENTS

LEARNING OBJECTIVES

Upon completion of this chapter, you should be able to do the following:

1. List the different types of terrorism methods.
2. List the six categories of terrorist threats.
3. Explain various types of safeguards against terrorism.

Terrorism is the use of tactics by small groups to create overwhelming fear, panic, or terror through the use of deadly force. Acts of terrorism are usually directed against specific or general targets in the general population and government. Generally, the goal of terroristic acts is to disrupt or destroy the bonds of trust and credibility between a government and its people. Sometimes the goals are to discredit or damage a group to achieve specific political aims.

Terrorism throughout the world is increasing each year. In 1980, the Federal Bureau of Investigation (FBI) classified terrorism as its third-ranking domestic bureau priority. Acts of terrorism directed at naval activities or installations have the potential to destroy critical facilities and to injure or kill key personnel. They can also impair or delay mission accomplishment or cause incalculable damage politically through adverse publicity and public perceptions.

The complexity of terrorism requires that you, as a second class petty officer, have a good understanding of terrorism. You must have the knowledge needed to protect yourself and to train your subordinates to protect themselves. This chapter will provide you with information on terrorism methods, threat conditions, and safeguards against terrorism.

TERRORISM METHODS

The record of terrorist activities directed at military activities in the past shows that terrorists might use the following methods:

1. **Bombing** —Bombing may be used to destroy equipment, cause fires, create casualties, and so forth. The bombs used may be of any degree of sophistication. Depending on bomb size and placement, the impact may range from a minor to a major crisis.

2. **Ambush** —Rapid ambush attacks are used by individuals or small groups to assassinate individuals, eliminate groups of naval personnel, or destroy or steal assets in remote locations.

3. **Armed Attack** —An armed attack, usually with one or more diversionary actions, is carried out by small groups against key personnel or critical assets on an installation. The objective is to disrupt the mission of the installation and to create adverse publicity. Normally, terrorists involved in this type of action take hostages only if their attackers try to prevent their escape.

4. **Hostage Seizures** —A terrorist group may seize a specific hostage or a number of hostages for ransom, media attention, coercion, or political bargaining purposes. The group may make an armed attack to seize critical assets (ships, submarines, aircraft, and so forth) manned with personnel. The terrorist group can then use the assets and personnel as leverage to bargain for publicity and political advantage.

5. **Sabotage** —Terrorist groups may use various sabotage methods to harass and demoralize personnel. Some of those methods include fires, explosive devices, mechanical devices, chemicals, psychological abuse, and unauthorized entries into computers.

TERRORIST THREAT TYPES

Terrorist threats are divided into the following six categories:

1. **Threat Type One.** One or more outsiders (nongovernment persons) who seek access to a base or restricted area or asset to perform an unauthorized act such as vandalism or theft

2. **Threat Type Two.** An individual or group, authorized access to a base or restricted area or asset, seeking to steal or remove an item of government property from the installation

3. **Threat Type Three.** A disgruntled employee seeking to perform an act of sabotage, data tampering, or wrongful destruction or otherwise destroy government property or impair mission accomplishment

4. **Threat Type Four.** An individual (outsider) or group seeking to make a political statement (antimilitary, antidefense, antinuclear, and so forth) by causing adverse publicity, usually nonviolent in nature, to embarrass the military service

5. **Threat Type Five.** An individual (outsider) terrorist, in philosophy and action, seeking access to a naval installation to commit an act of violence (sabotage, bombing, hostage abduction, murder, arson, or theft of sensitive matter including nuclear weapons, conventional arms, ammunition and explosives, and so forth)

6. **Threat Type Six.** A 2-to-12 person group of well-armed, well-trained dedicated terrorists seeking access to a naval installation to commit an act of violence (sabotage, bombing, hostage abduction, murder, arson, or theft of sensitive matter including nuclear weapons, conventional arms, ammunition, explosives, and so forth)

Commanding officers must have contingency plans to counter the six threat types. The following table summarizes the more sensitive areas and the threat types that must be included in a commanding officer's contingency plan.

AREAS	Under Normal Conditions Commanding Officers Must Have Ability To Counter Treat Types
Bases	1 2 3 4 5 6
Shipyards	1 2 3 4 5
Aviation (as an example, flight lines)	1 2 3 4 5
Waterfronts	1 2 3 4 5
Nuclear Weapons Storage	1 2 3 4 5 6
Communications Facilities	1 2 3 4 5
Intelligence Collection/Sensitive Communication Sites	1 2 3 4 5
Conventional Arms, Ammunition and Explosives Storage Sites	1 2 3 4 5 6
Bulk Petroleum, Oil, and Lubricants (POL) (ground fuels, POL war reserve, etc.)	1 2 3 4 5
Nuclear Weapons	1 2 3 4 5 6
Conventional Munitions	1 2 3 4 5
Small Arms (Armories)	1 2 3 4 5
Supply items	1 2 3 4 5
Funds and Negotiable instruments	1 2 3
Drugs, Drug Abuse Items	1 2 3 4
Precious Metals	2 3
Classified Information/ Material	1 2 3 4
Automatic Data Processing (ADP) Facilities	1 2 3 4
Aviation	1 2 3 4 5

THREAT CONDITIONS

Indications and warnings of terrorist activity against naval installations and personnel will

normally be received from U.S. security authorities. They may also be received through the security agencies of the host countries concerned. Information may also come from local police forces or be received directly by a U.S. command or agency as a threat or warning from a terrorist organization.

The declaration of a THREATCON, including the security measures it requires, may be decreed by a U.S. command or agency or by a local commanding officer or head of an agency following receipt of intelligence through official sources or following an anonymous threat message. The Alpha, Bravo, Charlie, and Delta THREATCONs are described in the following paragraphs:

Ž THREATCON ALPHA—This condition is a general warning of possible terrorist activity, the nature and extent of which are unpredictable. The circumstances do not justify the declaration of a THREATCON BRAVO.

Ž THREATCON BRAVO—This condition is declared when an increased and more predictable threat of terrorist activity exists even though no particular target is identified. The security measures required during this condition may have to be maintained for weeks without causing undue hardship, without affecting operational capability, and without aggravating relations with local authorities.

Ž THREATCON CHARLIE—This condition is declared when an incident occurs or when intelligence is received indicating that some form of terrorist action against an installation or personnel is imminent. The security measures required during this condition for more than short periods will probably create hardship and will affect the peacetime activities of the installation and its personnel.

Ž THREATCON DELTA—A terrorist attack has occurred or intelligence has been received that terrorist action against a specific location is likely. Normally, this THREATCON is declared as a localized warning.

Each naval installation or command provides instructions on the measures its personnel should take during each of the four THREATCONs.

THREAT ASSESSMENTS

Based on available information, your command must determine if the threat is going to be a short-, medium-, or long-term threat. Although the Naval Investigative Service (NIS) can supply those threat evaluations on request, they must be carefully analyzed to determine the required THREATCON level.

SAFEGUARDS AGAINST TERRORISM

Department of Defense (DOD) policy is to protect to the best of its ability DOD facilities, equipment, and personnel and their dependents from terrorist acts. Particular attention is given to informing and protecting high-risk targets. High-risk targets include the following:

- Key DOD personnel
- U.S. Military Assistance Advisory Groups (MAAGs) and other military missions
- Technical assistance field teams
- Training and advisory teams
- Defense attaché offices
- Nuclear weapons sites
- Recruiting offices
- Small communications, liaison, and administrative activities considered to be especially vulnerable to terrorist acts

Absolute protection against terrorist activities is impossible. Therefore, protective plans and procedures are based upon a balance between the degree of protection desired, mission requirements, and available manpower and fiscal resources.

The most cost-effective, broadly based method of organizing an antiterrorism effort is to integrate it as much as possible with crisis management procedures. Those procedures should set up ways to prevent, control, or contain natural and man-made crises. Essentially, specific antiterrorism

planning involves the use of two defensive measures:

1. Intelligence—Intelligence consists of information obtained through threat assessment and continuing contacts with the NIS or command intelligence personnel. An organization must have access to intelligence to prepare for or forestall terrorist incidents.

2. Target Hardening and Procedural Safeguards—Target Hardening and Procedural Safeguards consist of security measures established to protect critical and sensitive activity assets against terrorist threats. An organization's safeguards must present an increased cost and risk to professional terrorists.

Additionally, each of us plays active roles in safeguarding both property and personnel against terrorism. We should constantly be on guard against suspicious personnel, vehicles, and materials around our work facilities. We should report any suspicious personnel, vehicles, or materials to the security department.

SUMMARY

Acts of terrorism directed at naval personnel, activities, or installations have the potential to destroy critical facilities and to injure or kill personnel. They can also impair or delay command missions and cause incalculable damage.

This chapter provided information on terrorist methods, terrorist threat types, conditions, and assessments. By understanding those elements of terrorism, you are better prepared to assist in safeguarding yourself, other personnel, installations, and equipment against terrorist activity.

Be on the lookout for suspicious personnel, vehicles, and materials on and around your work facility. Call the Security Office if anything appears unusual or suspicious.

REFERENCES

Department of the Navy Physical Security and Loss Prevention, OPNAVINST 5530.14B, Chief of Naval Operations, Washington, D.C., 1988.

Protection of DOD Personnel and Resources Against Terrorist Acts, SECNAVINST 3850.1A, Secretary of the Navy, Washington, D.C., 1982.