Module 10

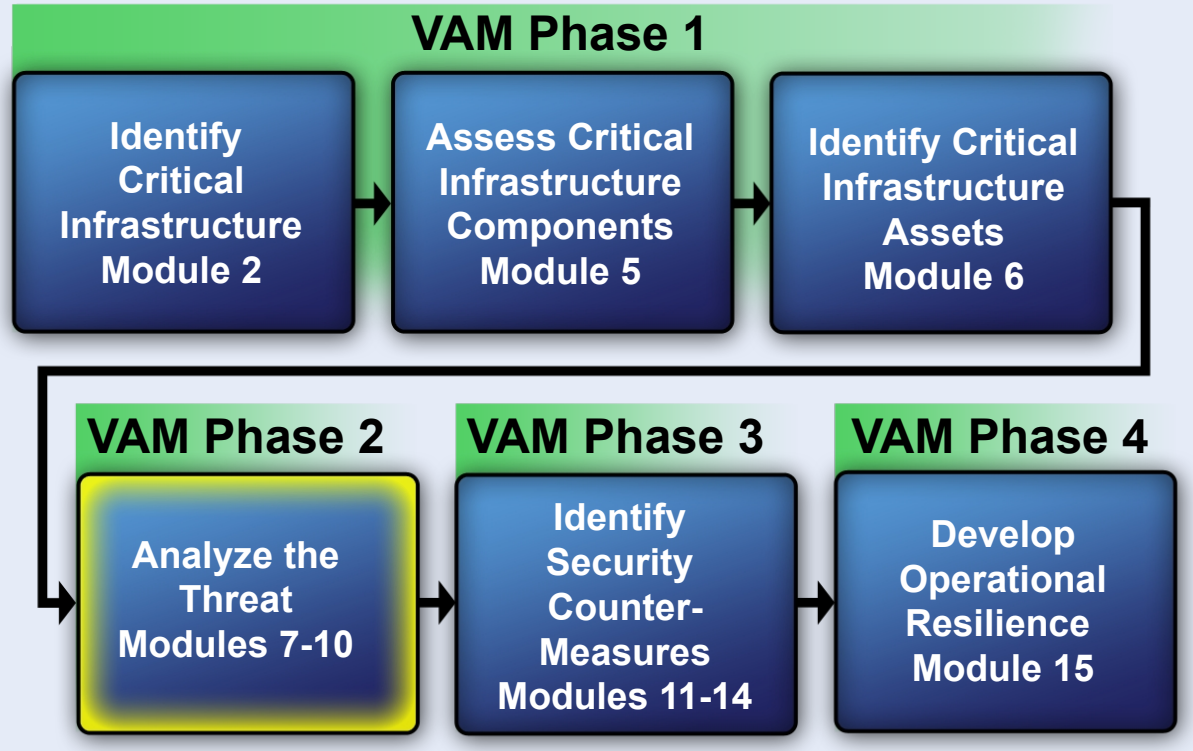
Analyzing the Threat

OFFICE OF ANTITERRORISM ASSISTANCE

Module Objective

- By the end of this module, you will be able to create a threat analysis statement for critical infrastructure

Physical Protection System



Purpose of the Threat Analysis

- Gather threat data
- Identify data sources
- Prepare threat analysis statement
- Establish physical protection system design requirements

Threat Analysis Statement (1 of 2)

- Identifies potential or credible threat capabilities
- Represents an assessment by informed and qualified people using available information


Source: FEMA.GOV

Threat Analysis Statement (2 of 2)

- Helps determine the basic requirements of a critical infrastructure's physical protection system
- Review and update as necessary

Sample Threat Analysis Statement Case Study (1 of 3)

Refer To:

Handout 10.1

- **Purpose: to examine and discuss a sample threat analysis statement from a given case study**
  - **Duration: 30 minutes (20-reading; 10-discussion)**
  - **Group composition: table groups**
  - **Debrief: large-group discussion**

Sample Threat Analysis Statement Case Study (2 of 3)

Refer To:

Handout 10.1

- Facility: nuclear power plant in Pelindaba, South Africa
- Specific threat: terrorist, radiological sabotage
- Credible threat: terrorist, theft, or diversion of special nuclear material

Sample Threat Analysis Statement Case Study (3 of 3)

Refer To:

Handout 10.1

- What critical information was not included in the sample threat analysis?
- What were some of the significant points of the threat analysis statement?
- What were some of the security countermeasure failures?

Potential Adversary Threats

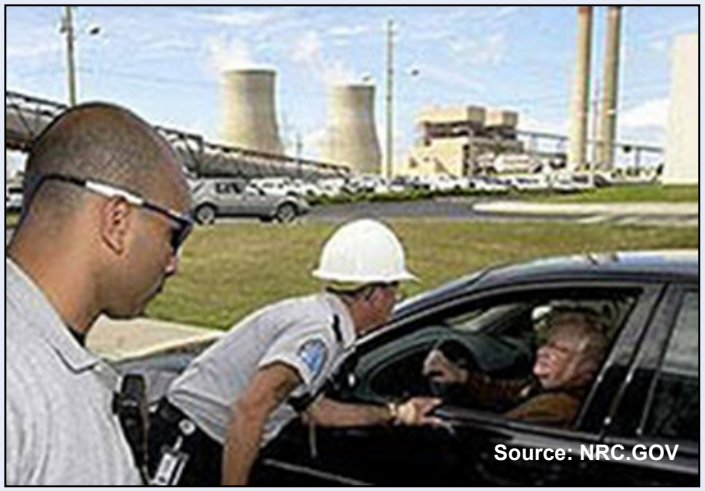
- This section will cover:
  - Adversary categories
  - Potential actions of an adversary
  - Adversary motivations
  - Adversary tactics
  - Adversary capabilities and limitations

Adversary Categories (1 of 2)

- Insiders — individuals with authorized access
- Outsiders — individuals without authorized access
- Insiders working together with an outsider

Adversary Categories (2 of 2)

- Terrorists
- Criminals
- Discontented employees
- Activists
- Mentally ill persons



Insiders

- **Most dangerous adversary because of:**
  - **Knowledge**
  - **Access**
  - **Opportunity**
  - **Motivation**
- **Includes:**
  - **Employees and contractors**
  - **Vendors and visitors**

Washington Navy Yard Shooting Case Study (1 of 2)

Refer To:

Handout 10.2

- **Purpose: to identify the threat involved in the case study**
  - **Duration: 10 minutes (5-case study; 5-discussion)**
  - **Group composition: table groups**
  - **Debrief: large-group discussion**

Washington Navy Yard Shooting Case Study (2 of 2)

Terrorists

- **Characteristics:**
  - Are motivated by political or social objectives
  - Conduct hostile surveillance
  - Plan to kill to achieve goals
  - Use explosives, automatic weapons, or both
  - Will risk capture, injury, or death
  - Target critical infrastructure

Criminals

- Often motivated by financial gain
- Develop financial networks to fund terrorist activity
- Seek to avoid either capture or detection

Discontented Employees (1 of 2)

- Perceived mistreatment by boss or disagreements with coworkers
- May disrupt known routines with aggressive behavior, theft, sabotage, or force
- May risk capture or detection

Discontented Employees (2 of 2)

- May use fear and intimidation
- May be an insider or an outsider with insider information

Activists

- Oppose ecological, political, and economic programs
- May use violent or nonviolent tactics for direct confrontation
- May attempt to defeat barriers (fences and walls)
- May be insider or outsider

Mentally Ill Persons (1 of 2)

- Known criminal with mental illness history or family history of violence
- Known member of a terrorist organization
- Appearance of being under the influence of alcohol or other drugs

Mentally Ill Persons (2 of 2)

- Undiagnosed mental illness with no outward signs
- May be insider or outsider

Discussion Question

- What are some examples of damage to critical infrastructure assets caused by terrorists, criminals, discontented employees, or mentally ill persons in your country?

Potential Actions of an Adversary (1 of 2)

- Consider the types of crimes and terrorist attacks these various adversaries are interested in and capable of carrying out
- Determine which of these acts pose a credible threat to the specific site
- Study historical examples and trends

Potential Actions of an Adversary (2 of 2)

- Sabotage — deliberate and malicious destruction or intrusion
- Theft — unlawful possession of property, equipment, or information
- Diversion of materials — unlawful movement or transfer
- Other violent acts — against critical people assets

Adversary Motivations

- Political
- Philosophical
- Social
- Economic
- Personal

Terrorist Tactics (1 of 2)

- Part of the threat analysis involves examining the tactics of each potential adversary
- Tactics may include or be a combination of:
  - Stealth — perform a task undetected

Terrorist Tactics (2 of 2)

- Force — gain access through the use of violence
- Deceit — provide false information to gain access

- Help enhance the design of the physical protection system

Adversary Capabilities and Limitations

- Determine system performance requirements
- Define threat more clearly
- Include specific considerations of:
  - Personnel
  - Knowledge, skills, and experience
  - Types and quantity of weapons
  - Tools and equipment
  - Transportation

TeachBack Moment

- Why is it important to analyze the threat?
- What are the different types of adversary threats?

Information Sources on Potential Threat (1 of 4)

- **Threat information helps define the threat:**
  - **The targeted critical infrastructure asset**
  - **Adversary's objective**

Information Sources on Potential Threat (2 of 4)

- Communication with organizations that can provide information
- Sources of threat information include:
  - Law enforcement reports
  - In-country intelligence reports
  - National threat data reports

Information Sources on Potential Threat (3 of 4)

- Military and law enforcement agencies
- International intelligence agencies

- Site incident reports
- Reports of criminal or terrorist activities in the area

Information Sources on Potential Threat (4 of 4)

- Contact lists for law enforcement activities
- Number and types of personnel at the facility
- Any available threat information

Discussion Questions

- What are other suggestions for sources of information about potential threats in your country?
- What types of similar sources of statistics on terrorist activities does your government have?

Organizing Threat Information

- Formats information to help facilitate the critical decision-making process:
  - Which threats should be included in the threat spectrum?
  - What is the effectiveness of the existing physical protection system?
- Includes both types of adversaries, insider and outsider, in the threat analysis statement

Barriers to Analytical Thinking (1 of 2)

Refer To:

Workbook 10.1

- An awareness of common barriers will help:
  - Avoid critical mistakes that could negatively affect critical infrastructure protection
  - Facilitate the analytical thought process relating to the physical protection system

Barriers to Analytical Thinking (2 of 2)

Refer To:

Workbook 10.1

- Focus on facts not personal opinions
- Use analytical thinking processes to overcome barriers

Discussion Questions

- In your experience, which types of barriers to analytical thinking have you encountered?
- What actions could you take to prevent or avoid these barriers?

Alternative Outcome Thinking Techniques

Refer To:

Workbook 10.1

- Advocating the opposite view
- Team A or Team B analysis
- Other team analysis
- “What if?” analysis
- High consequence and low probability analysis
- Outside-in-thinking
- Gaming and simulation

Insider Threat Information Worksheet

- Begin threat analysis by considering unique potential insider threats posed by insiders at the critical infrastructure facility
- Rate and organize the insider threat information on a worksheet


Source: DOL.GOV

Insider Threat Information Worksheet Activity

Refer To:

Workbook 10.2

- **Purpose: to help organize gathered information about insider threats**
  - **Duration: 15 minutes (5-reading; 10-discussion)**
  - **Group composition: table groups**
  - **Debrief: large-group discussion**

Outsider Threat Information Worksheet

Refer To:

Workbook 10.3

- Organized by an assessment of potential threat:
  - Actions
  - Motivations
  - Tactics
  - Capabilities

Outsider Threat Worksheet Activity

Refer To:

Workbook 10.3

- **Purpose: to help organize gathered information about outsider threats**
  - **Duration: 15 minutes (5-reading; 10-debrief)**
  - **Group composition: table groups**
  - **Debrief: large-group discussion**

Estimating Likelihood of Attack (1 of 2)

Refer To:

Workbook 10.4

- Determine information about each terrorist:
  - Threat type
  - Capability
  - History and intent
  - Target appeal (attractiveness)

Estimating Likelihood of Attack (2 of 2)

Refer To:

Workbook 10.4

- **Rating scale:**
  - Very Low
  - Low
  - Medium
  - High
  - Very High
- **Numerical scale to rate threat type: 1–10, with 10 being highest**

Estimating Likelihood of Attack Worksheet Activity

Refer To:

Workbook 10.4

- **Purpose: to provide an example to help you estimate the likelihood of attack of an identified threat**
  - **Duration: 25 minutes (20-activity; 5-debrief)**
  - **Group composition: table groups**
  - **Debrief: large-group discussion**

Steps to Prepare Threat Analysis Statement

Refer To:

Workbook 10.5

1. Compare the likelihood of attack for all threat types
2. Identify the most likely threat type
3. Prepare threat analysis statement

Preparing a Threat Analysis Statement Activity

Refer To:

Workbook 10.5

- **Purpose: to prepare a threat analysis statement using a given scenario**
  - **Duration: 15 minutes (10-activity; 5-debrief)**
  - **Group composition: table groups**
  - **Debrief: large-group discussion**

Community Engagement and Human Rights Discussion

- **Why is it important to engage the community in determining the types of threats that may exist?**

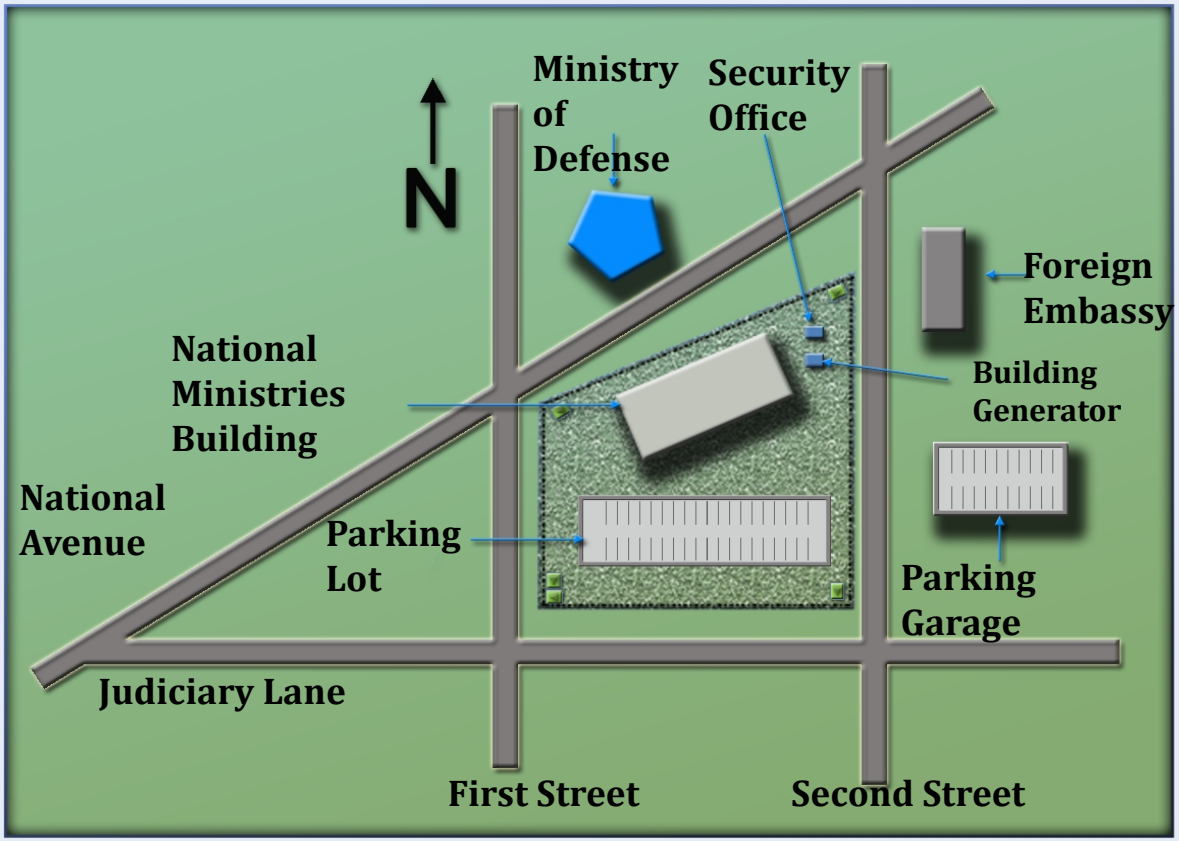
Threaded Exercise Part 3 — National Ministries Building

Refer to Workbook Part 3

- **Purpose: to prepare a threat analysis statement**
  - Duration: 60 minutes (45-exercise; 15-debrief)
  - Group composition: table groups
  - Debrief: presentation and discussion

National Ministries Building Complex Map

Refer to Workbook Part 3



Module Summary

- Purpose of the threat analysis
- Potential adversary threats
- Information sources on potential threat