LECTURE 8

PHYSICAL AND WATERSIDE SECURITY IN THE PORT FACILITY

MANAGING PHYSICAL SECURITY IN A COMPETITIVE PORT ENVIRONMENT

Physical security in seaports encompasses a range of resources and systems aimed at deterring crime and preventing unauthorized access by individuals, vehicles, or materials. While it is impractical to discuss every potential security measure, port security officers (FSOs) must focus on key physical security management aspects encountered daily. These include compliance with government regulations, adherence to industry standards, and ensuring that security measures support rather than hinder the port's operational goals.

Port operations are influenced heavily by market demands and competition among facilities. For example, ports along the southeastern U.S. coast—including Miami, Jacksonville, and Charleston—cater to overlapping shipping markets. If one port cannot accommodate an increase in container capacity or faces delays due to logistical issues, cargo operators can easily shift operations to another nearby port. Therefore, FSOs must balance implementing effective physical security measures with maintaining operational efficiency to remain competitive.

Security decisions at the ground level, such as gate access or credentialing requirements, can directly affect a port's clients. Overly restrictive measures may cause frustration among cargo operators, impacting the port's overall marketability. FSOs need to approach security from a holistic management perspective, considering how their actions affect operational fluidity and client satisfaction while staying compliant with legal and regulatory frameworks.

DEVELOPING STANDARD OPERATING PROCEDURES (SOPS)

An essential element of port security is the development and regular updating of the Facility Security Plan (FSP), which serves as a blueprint for mitigating identified risks. SOPs support the FSP by providing clear, practical instructions for staff to follow during routine and heightened security situations. These procedures ensure consistency, compliance with regulations, and effective implementation of security strategies.

Key areas requiring SOP documentation include:

- Security committee operations.
- Crime, terrorism, and vulnerability assessments.
- Guard force protocols.
- Emergency response planning.
- Communication with law enforcement agencies.
- Access control and credentialing systems.
- Visitor management in restricted areas.

- Information security.
- Firearms and weapons restrictions.

By providing staff with detailed guidance, FSOs ensure that security measures are effectively implemented while minimizing risks associated with operational disruptions or potential liabilities.

PERIMETER SECURITY

Perimeter security involves detecting, assessing, and responding to threats along the port's boundaries. Effective strategies depend on the facility's unique layout and location, incorporating a mix of physical barriers, technological tools, and procedural controls. For example, PortMiami's location on an island near a major metropolitan area requires careful consideration of roadway connections, waterways, and urban infrastructure.

Planning perimeter security should prioritize the integration of natural features, technology, and human resources to deter unauthorized access. Hardware decisions, such as fencing or alarm systems, should follow a thorough assessment of the port's operational needs and vulnerabilities.

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)

CPTED principles focus on designing environments to reduce crime by influencing human behavior. The following strategies can enhance perimeter security:

1. **Natural Surveillance:** Maximizing visibility through lighting, open layouts, and clear sightlines deters potential intruders.
2. **Natural Access Control:** Defining public and private spaces with clear boundaries and pathways increases perceived risks for unauthorized access.
3. **Territorial Reinforcement:** Landscaping, fencing, and design elements create a sense of ownership and discourage intrusion.
4. **Maintenance:** Regular upkeep of the facility, including repairs, landscaping, and lighting, reinforces the perception of active surveillance and control.

Applying CPTED principles ensures that security measures align with the port's operational and environmental context.

FENCING

Fences are critical for defining boundaries and discouraging unauthorized access but are often insufficient as standalone deterrents. FSOs must evaluate the most suitable fencing types based on the port's operations and risks. Common options include:

1. **Chain-Link Fences:** Durable and economical, these are effective for visual deterrence. Smaller mesh openings can prevent contraband transfer. In high-risk areas, double fencing may be used to create additional security layers.

2. **Barbed Wire:** Typically added to the tops of fences to deter climbing, barbed wire must be installed at appropriate heights to maintain effectiveness.
3. **Concertina Wire:** This flexible, sharp-edged wire adds another layer of defense, particularly when placed at the top or bottom of fences.

Fencing systems should be regularly inspected for damage and reinforced where necessary. In some cases, barriers or wall-fence combinations may provide greater resilience against breaches or operational wear. Alarm systems integrated with fences can further enhance security but must be calibrated to minimize false alerts caused by environmental factors.

Professional standards, such as those outlined by ASIS International, provide guidance on appropriate fence heights and materials based on the level of security required. FSOs should reference these standards while tailoring fencing strategies to their facility's specific needs.

PARKING CONTROL MEASURES IN PORT FACILITIES

Effective parking control serves as a critical layer of physical security in port facilities, aiding in the management of vehicle access and movement. Ideally, parking zones should be positioned outside of fenced operational and restricted areas. This arrangement minimizes the risks of unauthorized cargo transfers or smuggling of contraband. By keeping personal vehicles away from cargo and operational spaces, security is enhanced, and illicit activities are deterred.

Enforcing parking regulations is a key responsibility of the Port Facility Security Officer (FSO). Ensuring compliance helps prevent vehicles from being misused to transport stolen goods or prohibited items. However, the challenge of enforcing parking controls can be significant due to space constraints and operational requirements at many ports. In some cases, vehicles may need access to operational areas for specific tasks, such as crane maintenance, safety equipment transport, or immediate responses to emergencies.

For ports with substantial cargo operations and numerous employees requiring access, solutions may include offsite parking with shuttle services or employee-only bus systems, similar to practices at airports. Security protocols should also require employees to pass through controlled checkpoints when leaving restricted areas, with port security staff overseeing these transitions. Regular vehicle monitoring and staff movement tracking serve as an added deterrent against illegal activity.

Employees should notify management or security personnel before visiting vehicles during work hours. Restrictions on vehicle access to operational zones, coupled with a permit system for parking, allow for better oversight. Credentialing and identification of all vehicle owners further bolster security. A robust enforcement strategy—incorporating measures like warnings, fines, or towing—sends a clear message about the importance of compliance with parking regulations. Ultimately, fostering cooperation between the port community and management enhances overall security.

MANAGING ACCESS POINTS

Optimizing access points in port facilities is a delicate balance between security and operational efficiency. While fewer access points may improve security, they can hinder port operations, deterring potential customers. Conversely, an excessive number of poorly managed access points increases the risk of unauthorized entry and demands more resources for monitoring.

This balance can be achieved through comprehensive risk assessments, threat analyses, and careful infrastructure planning. Collaborative efforts between port FSOs, operational staff, and development teams are crucial to determining access point placements and functionalities. For instance, cargo-focused ports must accommodate large trucks by implementing credentialing systems, multiple lanes, and secure gates. Separate entryways for pedestrians and vehicles ensure safety and enable focused security screening.

Access points should be continually evaluated and secured. Gates that are unused should be sealed to prevent unauthorized entry, while high-use gates should feature strong locking mechanisms, such as reinforced chains or deadbolts. Incorporating recording systems to track inspections or patrols adds accountability and ensures consistent gate security. Alarms and other advanced security measures may be required for sensitive areas.

Gatehouses should be equipped with essential utilities, including power, communication devices, and credentialing systems, to enable seamless security operations. Additional barriers, such as bollards, gate arms, and metal teeth, can enhance security. Ports facing frequent changes, like construction or berth shifts, can use movable concrete or water-filled barriers as temporary solutions.

ADDRESSING SMALL VESSEL THREATS AND WATERSIDE SECURITY

The potential threats posed by small vessels to maritime security have long been a concern. With millions of registered recreational and commercial vessels operating near critical infrastructure, the risks are complex and multifaceted. These risks include smuggling, unauthorized access, and the use of vessels as platforms for attacks.

The U.S. Department of Homeland Security identifies small vessels as those under 300 gross tons, such as fishing boats, recreational crafts, and small commercial ships. Their mobility and limited regulation create challenges in tracking and monitoring their activities. For example, there is no centralized system for vessel registration, and documentation requirements vary widely across states.

Key vulnerabilities include their proximity to critical infrastructure, limited tracking capabilities, and a lack of universal regulations. To address these concerns, the U.S. government emphasizes a collaborative approach, engaging federal, state, and local authorities, as well as private stakeholders. Strategies include enhancing public awareness, improving reporting mechanisms for suspicious activities, and leveraging advanced technologies to detect potential threats.

The Department of Homeland Security's Small Vessel Security Strategy outlines four main objectives:

1. Strengthening partnerships with the small vessel community to increase maritime domain awareness.
2. Implementing layered security approaches to enhance safety and deterrence.
3. Utilizing technology to detect and address risks posed by small vessels.
4. Fostering collaboration between public and private entities to ensure cohesive responses.

Ports and waterways can benefit from increased boater education, systematic risk assessments, and enhanced patrol capabilities. With robust enforcement of safety regulations and a culture of vigilance, stakeholders can work together to mitigate the risks associated with small vessels while preserving their essential role in maritime activities.

MITIGATING SMALL VESSEL THREATS IN PORT SECURITY

Domestic seaports employ various strategies to detect and manage potential security threats posed by small crafts in their waters. Key insights were identified during the 2007 National Small Vessel Security Summit, highlighting methods such as enhanced intelligence collection, situational awareness, and rapid threat detection.

STRATEGIES FOR SMALL VESSEL THREAT MITIGATION

» Neighborhood and Public Awareness Programs

These initiatives foster vigilance among local communities, encouraging reporting of suspicious activities.

» Advanced Surveillance Technologies

Wide-area surveillance systems, including radar, sonar, and infrared technologies, can help detect and monitor small crafts effectively.

» Explosive and Suspicious Material Detection

Standoff detection systems can identify potential threats such as explosives or components of weapons of mass destruction (WMD).

» Enhanced Monitoring and Investigation

Proactive measures include monitoring small crafts and swimmers, detecting suspicious materials, and conducting investigations into unusual activities.

RAPID THREAT RESPONSE

Quick interdiction strategies are essential to neutralize potential threats efficiently.

ACCESS CONTROL AND INTERDICTION

Effective threat mitigation relies on controlling access to port facilities. This includes:

- Deploying non-lethal disabling technologies.
- Ensuring robust interagency coordination.
- Enhancing information sharing and private-sector collaboration.

» Federal Regulations and Standards

The Maritime Transportation Security Act (MTSA) of 2002 mandates U.S. ports to implement continuous security measures. Facilities must monitor their surroundings using a combination of lighting, security personnel, patrols, and surveillance equipment as detailed in their Facility Security Plans (FSP). These measures encompass:

- The facility and its approaches (land and water).
- Restricted areas within the facility.
- Vessels docked at the facility and nearby zones.

DOMAIN AWARENESS STRATEGIES

Adopting domain awareness systems enhances situational awareness. Examples include:

1. **Intrusion Barriers**
   Floating barriers prevent unauthorized small craft access and support surveillance equipment.
2. **Waterside Surveillance Systems**
   These integrate multiple technologies and require significant infrastructure investment tailored to the port's needs.
3. **Shore-Based Patrols**
   Stationary and mobile patrols provide human oversight on docks, seawalls, and other critical areas.
4. **Waterborne Security Patrols**
   Ports deploy armed security personnel using specialized boats tailored to local operating conditions.
5. **External Marine Patrols**
   Collaborations with law enforcement agencies enable inspections of underwater dock areas, vessel hulls, and infrastructure support columns.
6. **Restricted Waterway Access**
   Policies limiting waterway access to authorized vessels enhance security.
7. **Diver Operations**
   Divers inspect below-water structures for tampering or suspicious devices.

COORDINATED SECURITY RESPONSIBILITIES

Before 2001, port waterside security was managed by various public and private agencies.

Following MTSA's enactment, the U.S. Coast Guard emphasized that port facilities themselves should assume responsibility for waterside security, incorporating marine patrol assets into their FSPs.

PERIMETER AND PHYSICAL SECURITY

Ports employ a combination of physical and technological measures to secure their perimeters. These include:

- Intrusion detectors, alarms, and barriers.
- Surveillance cameras and radar systems.
- Strategic fencing to define boundaries and deter intrusions.
- Parking controls to regulate vehicle access.
- Clearly marked exclusion zones and signage to prevent unauthorized entry.

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)

CPTED principles aim to influence human behavior through:

- Natural surveillance and access control.
- Territorial reinforcement.
- Defensible space strategies to design safer facilities.

SMALL VESSEL THREAT CATEGORIES

Small vessels, defined as crafts under 300 gross tons, pose risks in four main categories:

- Waterborne improvised explosive devices (IEDs).
- Weapons smuggling.
- Transporting terrorists.
- Platforms for launching standoff weapons.

U.S. SMALL VESSEL SECURITY STRATEGY (SVSS)

The SVSS promotes collaboration among federal, state, and local authorities, international partners, private industries, and recreational users to:

- Enhance maritime domain awareness.
- Utilize layered security measures.
- Leverage technology for threat detection.
- Foster public-private cooperation.

RECOMMENDATIONS FOR PORT SECURITY OFFICERS (FSOS)

Port FSOs must:

- Evaluate local and federal marine security zones.
- Coordinate with the U.S. Coast Guard and other agencies.
- Develop scalable security measures tailored to their facility.

- Ensure robust waterborne patrol capabilities.

Key considerations for patrol boat specifications include:

- Minimum length: 23 feet.
- Dual engines with at least 200 horsepower.
- Advanced navigation and communication systems.
- Comprehensive safety and surveillance equipment.

// CONCLUSION //

Seaports must balance operational efficiency with robust security measures to protect their waterside perimeters. By integrating physical security devices, advanced technologies, and collaborative strategies, port FSOs can effectively mitigate small vessel threats and ensure maritime safety.