First in a Series

PORT SECURITY:
A National Planning Guide

U. S. Department of Transportation

1997

Introduction

Port Security: A National Planning Guide has been produced for the purpose of conveying the United States Department of Transportation's policy perspective on port security to the maritime community. This guide provides an overview of the essential aspects of port security and identifies many of the challenges facing ports. It is also intended to provide local governments and the commercial maritime industry with a common basis upon which to establish port security standards and the outcomes expected from meeting those standards.

This guide is intended to be the first document in a series to be produced through the cooperative efforts of the maritime industry and the Federal government. The guide and subsequent technical manuals are intended to be usable by port directors or general managers, the directors of port security, and the officers of port security departments in fulfilling their responsibilities toward the development of an effective port security program.

The subsequent technical manuals will be sufficiently detailed to serve as "how to" manuals for planning and conducting the daily operations of port security. These manuals will include outcome based goals and measures of effectiveness. This can enhance the ability of port security managers to execute their risk management responsibilities and to measure the impact and effectiveness of the security measures implemented in the port. These manuals are expected to address such topics as:

* Developing and Implementing a Security Plan

* Security Survey and Risk Assessment

* Physical Security and Access Control

* Information Security

* Personnel Security

* Maritime Terrorism

* Drug Smuggling

* Stowaways and Alien Smuggling

* Roles/Responsibilities/Legal Authorities of Port Agencies

* Sea Robbery

* Cargo Security and Hazardous Materials

* Intelligence

This guide and its subsequent technical manuals are intended to be dynamic, and therefore flexible enough to be revised so that they may remain current and useful. The manuals will provide guidance and processes which can be selected, combined and adapted to meet the unique needs of a given port. In this way, consistent port security objectives can be maintained, enabling government and the commercial maritime industry to achieve them, regardless of changes in circumstances and technology.

This document was produced by the U.S. Maritime Administration and the U.S. Coast Guard under the direction of the Department of Transportation's Office of Intelligence and Security. In developing this guide, input and contributions were sought and received from the maritime community and other federal agencies.

Comments or questions on the information in this guide should be made to either the Coordinator, Maritime Intelligence & Security, Office of Ports and Domestic Shipping, Maritime Administration, U.S. Department of Transportation, 400 Seventh Street, SW, Washington, DC 20590, or telephone (202) 366-5473/fax (202) 366-6988; or Chief, Response Operations Branch, U.S. Coast Guard, 2100 Second Street, SW, Washington, DC 20593-0001, telephone (202) 267-0518/fax (202) 267-4085.

Federico Peña

Secretary of Transportation

Table of Contents

Introduction

Table of Contents

Maritime Security
- Maritime Security Today
- The Cost
- Responding to the Threat
- Industry/Government Partnership
- Planning For Port Security
- Association of Port Security Directors

Fundamentals of Port Security
- Port Security Goals and Principles
- Port Management and Security Planning
- Port Security Planning Cycle
- Security Survey and Risk Assessment
- Port Security Plan

Port Security Operations
- Implementation of the Port Security Plan
- Port Security Measures and Procedures
- Physical Access Control
- Information Security
- Port Security Training
- Personnel

Threats and Issues Facing Port Security
- Maritime Terrorism
- Sea Robbery
- Cargo Theft
- Stowaways and Alien Smuggling
- Drug Smuggling
- Currency Smuggling

Future Challenges

Technology and Innovation
Intelligence Data Bases
Electronic Data Interchange
Satellite Tracking of Cargo
Privatization
Port Congestion
International Cooperation

Conclusion

Recommended Readings

Maritime Security

Worldwide, maritime cargoes and vessels are increasingly targeted by organized criminal conspiracies or individuals involved in alien smuggling, cargo theft, drug smuggling and terrorism. Exploiting weaknesses in port security is central to these crimes. The associated costs reduce the competitiveness of those affected, including the ports. So long as threats to trade exist, port security will remain as essential to port operations as cargo and good labor relations.

Maritime Security Today

Traditional views of port security responsibilities must be expanded. A complex transnational set of security issues threaten the maritime industry and the movement of cargo in international trade. Those threats include terrorism, piracy, smuggling of stowaways and drugs, cargo theft and fraud, bribery and extortion. Sea robbery provides an excellent example of the complexity of port security issues. The nature of sea robbery necessitates that port security controls include both the waterside and the land side access of ports. However, jurisdictional authority discrepancies, a lack of financial resources, and equipment problems are frustrating the attempts by some countries to address this issue.

Enacting requisite port security measures and coordination, cooperation, and communication with government and maritime industry components are necessary. Solutions require multinational participation from governments and the international commercial maritime industry. The international trade community and constituents of the world economy in general must also become partners in this responsibility.

The Cost

In addition to direct financial losses due to maritime crime, the total cost includes an impact on productivity, possible loss of life, rehiring, retraining, and time spent with police, attorneys, claim adjustors, and the news media. Real costs also include increased insurance costs, liability exposure and the loss of trade as well as the loss of goodwill and reputation.

Responding To the Threat

Port security is an essential part of the safe, secure, and competitive operation of the maritime transportation system. It promotes the development of commerce and is an essential element in maritime trade competitiveness, which cannot be achieved merely by modernizing port infrastructure and increasing operating productivity.

Port security can surface as a significant issue in trade negotiations and government and industry courses of action should be coordinated to facilitate effective solutions. Port authorities should develop the means for exchanging current information on port security issues and for the dissemination of intelligence to the commercial industry. Through this approach, the security programs of individual ports can be enlarged into a national alliance of many port security programs working cooperatively with all elements of the maritime industry.

Industry/Government Partnership

Cooperation of industry and government is necessary to address the complex issue of maritime security. To achieve cooperation, the security departments of seaports must develop partnerships with law enforcement and the transportation industry's shippers, carriers, and insurers.

Profitable port business and trade relationships are dependent upon the security of the trade corridors through which a port's business is conducted. The scope of port security, therefore, extends beyond the physical facilities of the port to include the other ports, shippers, intermodal transportation carriers, insurers, etc., moving cargo and passengers through an interdependent trade network. Through cooperative partnerships, an economy of effort can be achieved while actually increasing the degree of security provided to all aspects of the maritime transportation system.

Planning For Port Security

Port security must be included in the national transportation planning framework that establishes priorities for allocation of resources for governmental and private funding of infrastructure investments. Security operations should be considered in the earliest planning and design phases for the construction and restoration of port infrastructure in order to achieve an operational environment designed to limit opportunities for criminal exploitation.

Association of Port Security Directors

The establishment of an association of port security directors in trading regions is recommended. Each association would serve as a forum for facilitating periodic analyses, discussion, recommendations, and mutual assistance. The association would be self-managed and conducted in a fashion common to such organizations, with a documented charter, a board of directors, and officers rotated by election. The association would work toward the common benefit of its member ports, and confer with other such associations on an inter-regional basis.

Fundamentals of Port Security

Port Security Goals and Principles

The goal of port security is to establish an environment in which trade may be conducted with reasonably high assurance of being unencumbered by criminal activity and without becoming a conduit for such activity. A port security department should strive to constrict the opportunities for criminal exploitation of the maritime transportation system, its providers and users. In developing a security program, the emphasis should be placed on deterring, preventing, detecting, and reducing the losses attributed to criminal activities. In order to do so, port security operations must be proactive rather than merely reactive. This requires intelligence and investigative coordination with law enforcement agencies and the security departments of the maritime industry companies utilizing a port's facilities.

Port security must also be capable of assessing threats to the port, and responding appropriately to those threats. Therefore, the port security department must be proactive in its thinking rather than reactive. Port security must employ all forms of intelligence information, promote awareness within the port community, conduct training, practice preparedness, and exercise security plans. The goal should be to identify processes and procedures that can be implemented while adapting to a changing environment.

Port Management and Security Planning

Port security must become a planning priority in port operations, commanding the attention and resources of senior port management. While responsibility and accountability for port security goals and principles rest with the director of the port,

the manager of the port security department, and the officers of the port security force, all persons within the port community must undertake a commitment to its implementation and success. The port's mercantile operations of moving cargo and passengers are especially sensitive to the effectiveness of security operations.

Port operations and security at a marine terminal involve extensive and detailed planning considerations that must be coordinated with the port's security program. There must be a level of consistency between a port's operational policies and procedures and its security program. Effective port security is achieved by integrating port planning and operations functions with port security. In this way, the port's business and security goals are developed through a planning process involving mutual perception of requirements. It is through this planning and coordination that the successful implementation of a port's security plan and the operational objectives are achieved.

Port Security Planning Cycle

Essential to port security planning is the ability to document and measure evidence of security threats, vulnerabilities, loss control, and the success of security measures implemented. This necessitates a system for monitoring implementation results and evaluations as a continuing process for improving a port's security effectiveness. The identification of these measures is critical to a port security service gaining budgetary and organizational support.

A security planning cycle is both strategic and tactical in nature, making it a dynamic process subject to adjustment as operational circumstances demand. The element of change necessitates that the security planning cycle be a continuous process. It requires intelligence information inputs to analyze security threat conditions, as well as an assessment of vulnerabilities and an evaluation of the suitability of security countermeasures being implemented.

Security Survey and Risk Assessment

Ultimately, the port security planning process must develop and implement measures to reduce port vulnerabilities. Unless there is recognition of potential vulnerabilities, appropriate countermeasures cannot be developed. Port security management must be capable of ascertaining the nature and magnitude of all foreseeable security threats to the port's operations. Consequently, a comprehensive security survey is the first task in the process of establishing an effective port security regime.

The security survey should be comprehensive in order to enable a complete and accurate analysis of the port's vulnerabilities. In addition to identifying the current and potential vulnerabilities to which the port's operations are exposed, it should be compiled in a manner that makes it possible to measure the frequency and severity of exploitation of those vulnerabilities. Analysis of the information compiled in the survey will assist in the selection of various security measures to best counter potential losses and to monitor the effectiveness of countermeasures.

Port Security Plan

All port authorities should establish and implement a comprehensive port security plan and associated policies and procedures. Further, the plan should be exercised by the port on a regular basis. In developing the plan for implementing port security operations, the following criteria should be considered: (a) the port's vulnerability to potential threats, (b) the effect of security measures on the port's efficiency and

operations, practical limitations imposed by physical characteristics of port infrastructure, (d) availability of funds, (e) alternative measures available, and (f) evaluation of all available security capabilities, internal and external.

Where applicable, the elements of a port security plan should be carried out in coordination with such entities as the nation's coast guard, customs service, port authority, local law enforcement authorities, harbor master, marine terminal operators, etc. Documentation for these activities should be part of the port security plan, and should be integrated and consistent with the other portions of the plan pertaining to standards.

Port Security Operations

Implementation of the Port Security Plan

One of the keys to successful implementation of any port security program is support of senior management. Another key is the commitment of port personnel. Port personnel will generally be more interested in the successful implementation of a security plan if senior management has authorized and supports its development. A third key is integration of security into the port's overall management, planning, and operations.

The operations of ports worldwide are similar; however, each has its own unique activities and trade circumstances. These differences affect not only the vulnerabilities of a port but the countermeasures that should be implemented. It is essential that port management and staff be directly and thoroughly familiar with the port's facilities, operations, and plans. Accomplishing this requires a cooperative working relationship between security personnel and personnel responsible for the port's general management and operations.

Port Security Measures and Procedures

The tactical responsibilities of port security apply to the vessels, cargoes, passengers, and the installations of the port facility itself, such as buildings, equipment, and trade information. The measures and procedures employed, therefore, must be adequate to counter the threat within the context of the physical port facility and its operational environment.

The essential components of port security measures and procedures should be structured to include land side operations and marine patrols in the harbors, anchorages, and waterways of ports to: (a) control access to the port, its installations, and vessels, (b) control access to cargo or passengers while in the port, © prevent sabotage to vessels calling at the port, to port facility installations, and to the port's business and trade information systems.

Physical Access Control

The importance of controlling the physical access to the port facility, its installations, and cargo is paramount. Once physical access has been achieved by criminals, cargo can be stolen or subjected to various forms of exploitation. In addition to exploiting cargo, other illicit activities can occur within the port. These activities may include smuggling of weapons, drugs, currency, contraband goods, and stowaways, or even the placement of an explosive device within a containerized shipment. Further, breaches in security that allow criminals electronic access to cargo documentation makes criminal exploitation easier, particularly with the collusion of seemingly legitimate companies fronting for criminal enterprises.

Port security operations may necessitate the ability to take up positions at all entry points, open storage areas, and warehouses throughout the port and inspect the

identification papers of arriving workers. It may also include being capable of controlling the movements of trucks transporting cargo through the port, and searching containers, warehouses, and ships in port as well as in the anchorage awaiting a berth.

Information Security

Port security must be prepared to counter not only threats posed by physical access to a port but also access to information. Unauthorized access to information used by a port in the conduct of its business can be exploited just as effectively as access to the port itself.

Access to information, such as the contents of containers, is a growing problem in the area of maritime security. Port security programs must address methods and procedures for ensuring information security.

Port Security Training

Lack of training is one of the most common deficiencies in any security organization. A marine terminal may increase its liability exposure not only for failing to implement reasonable security measures but for failing to properly train its personnel in effective security measures.

Becoming effective in implementing port security measures and procedures requires competent training. Training of the port security force and supervision of daily security operations are two of the most important responsibilities of port security management.

Training should include programs to train the trainer. This action creates a force multiplier effect that will in turn produce more security-trained port officials. Port security departments should seek the establishment of regional port security training centers with cooperation of national and international organizations, where port officials, law enforcement, and customs personnel can receive training.

Personnel

The true base of any security program will be the personnel selected to institute that program. Port organizations must make those efforts necessary to ensure that the port's security personnel are a competent and professional force. While many of the items mentioned earlier in this section will assist in the development of competencies within personnel, ports must also consider the level of professionalism that they desire of their security personnel. This will include such items as making a determination on whether security personnel should be sworn law enforcement officers and conducting background checks on personnel before hiring. Port management must also make the security personnel aware of their importance to the successful operations of the port.

Threats and Issues Facing Port Security

Internationally, port cities and their surrounding areas are experiencing dramatic increases in various forms of maritime crime, such as the theft and in-transit hijacking of entire containers and trailers and the smuggling of drugs and migrants. Maritime crime is being committed by highly organized and sophisticated criminal groups with the ability to exploit the international commercial shipping trades. Port security

departments must be prepared to counter the various international security threats. The characteristics of several of those security threats and issues are described below.

Maritime Terrorism

Port security must have an anti-terrorist component to contend with the possibility of a terrorist attack directed against port facilities and vessels within a port's jurisdiction or the territorial waters of the state. As is true with other port security programs, any anti-terrorist planning or implementation will necessitate extensive coordination with governmental authorities at the national and, possibly, international levels.

At a minimum, an essential function for port security is the dissemination of warning information to alert users of the port to the threat of terrorist activities. Such advisories elevate awareness regarding terrorist threats and focus the attention of the maritime industry on increasing its own security posture during the period of warning.

Information of potential terrorist activity will most likely originate from national or international governmental authorities in law enforcement or intelligence agencies. Port security should be involved in the response system at least to the extent necessary to alert and protect the community of port users.

Port security should be active in working cooperatively with ocean, truck, and rail carriers and other port users to establish anti-terrorist response capabilities in advance of the need. Port security services should include assisting with the review of vulnerabilities pertaining to shipboard and terminal security plans and contingency response procedures for both freight and passenger trades.

Dissemination of warning information to the maritime industry by the U.S. Government, for example, is effected through the coordination of its organizations. They are the U.S. Government's Department of State, Maritime Administration, Coast Guard, Office of Naval Intelligence, Secretary of Transportation's Office of Intelligence and Security, and Defense Mapping Agency.

Sea Robbery

Sea robbery is a term used to describe attacks upon commercial vessels in ports and territorial waters. Such attacks are, according to international law, not true acts of piracy but rather armed robberies. They are criminal assaults on vessels and vessel crews, just as may occur to truck drivers within a port area. Such attacks pose a serious threat to trade. The methods of these attacks have varied from direct force using heavy weapons to subterfuge in which the criminals have identified themselves on VHF radio as the national coast guard.

These maritime criminals are inclined to operate in waters where government presence is weak, often lacking in both technical resources and the political will to deal effectively with such attacks. International law permits any warship or government vessel to repress an attack in international waters. In a state's territorial waters, such attacks constitute an act of armed robbery and must be dealt with under the laws of the relevant coastal state. These laws seldom, if ever, permit a vessel or warship from another country to intervene. The most effective countermeasure strategy is to prevent criminals initial access to ports and vessels, and to demonstrate a consistent ability to respond rapidly and effectively to notification of such a security breach.

Cargo Theft

Cargo theft has become a growing problem in many countries and the transnational character of cargo theft is becoming increasingly evident. Investigations have linked criminals involved in cargo theft with transnational drug trafficking and money laundering activities. Cargo theft can become so severe a problem in a country as to constitute a serious threat to the flow of commerce. In the United States, for example, cargo theft losses are estimated to exceed $10 billion, with the value of a single cargo theft averaging about $500,000.

To effectively counter cargo theft and truck hijacking, port security personnel must be thoroughly familiar with the port's physical facilities and the operations of its terminals. They should also be aware of the details of cargo handling operations scheduled for the day, including berths, ships, and times. Further, there is a need to be closely familiar with the names of trucking companies, warehouse operators, and drivers doing business with the port, in addition to their practices and reputations. Hijackers acting with apparent information about the cargo manifests suggests that collusion is occurring at the intermodal freight interchange points.

Another element needed to combat this threat is a comprehensive data base of cargo loss compiled through a formal system of reporting and analysis. This is an essential analytic tool for reducing theft-related losses in the maritime industry. These data bases are needed in each country in order to develop a comprehensive assessment of the problem. The lack of such a data base has been an obstacle to effective cooperative action by the industry, local law enforcement, and government agencies.

Stowaways and Alien Smuggling

Stowaways jeopardize the integrity of international maritime commerce. The risk for ports and ocean carriers is being elevated by the increased use of containers in organized criminal conspiracies to smuggle transnational migrants. Adding to that risk is the migration of millions of people worldwide, impelled by various motivations. The volume of migrants is increasing the percentage of those likely to become ocean stowaways to escape their situation. Stowaways result in service disruption and revenue losses for vessel operators, which typically are held legally responsible for repatriation.

Port security must be capable of preventing stowaways through physical access controls at terminal facilities in port areas and at vessels, at warehouses, and at cargo storage areas. The methods of operation employed to smuggle stowaways aboard ship are strikingly similar in ports worldwide. However, sophisticated smuggling efforts are placing stowaways in containers during the freight forwarding phase, before delivery to the marine terminal, thereby increasing the challenge to port security.

Complicity of corrupt port and vessel personnel enabling stowaways access is a crucial issue with which port security must contend. Stowaways are gaining access to ships disguised among, and aided by, crews of legitimate port workers. Stowaways may board vessels as part of stevedoring crews or with others who have port and vessel access. Adding to the difficulty of identification, stowaways may carry fraudulent documents, such as passports and visas.

Drug Smuggling

Ports are vulnerable to being used by sophisticated smuggling schemes which rely on concealment of narcotics in shipments of commercial containerized maritime trade.

Smugglers are utilizing front companies or exploiting legitimate shippers in the process.

A port must accept responsibility for ensuring or taking the steps necessary to prevent its facilities from being used by drug smugglers. Included in this responsibility are physical security measures such as access controls, lighting, and patrols of the port.

There must also be a coordinated effort with those shipping companies using the port's facilities. This may include agreements to either have the ship operators conduct a vessel search for drugs or a cooperative search of the vessel by the ship's crew and port security personnel. Additionally, contacts should be made with various enforcement authorities to obtain assistance and intelligence that can be used in helping them curtail drug smuggling operations from a port's facilities.

The growing volume of containerized maritime trade also provides opportunities for smuggling illicit drugs and the precursor chemicals used in the manufacture of drugs such as cocaine and heroin. Concealment of illicit shipments manifested as legitimate commercial cargoes, and the diversion of legal chemicals following legitimate transactions by unscrupulous shippers is a serious problem. Port security should include controls on precursor chemicals shipped through the port and be able to implement methods and procedures for investigating the theft or diversion of precursor and essential chemicals. Availability of auditable documentation of chemicals and their producing companies throughout their shipping cycle within the port is of crucial importance.

Currency Smuggling

Currency smuggling is an integral component in the money laundering process and the accumulation of illegitimate wealth. Organized crime uses that financial power to corrupt officials, infiltrate legitimate business through legal purchases and criminal means, and create monopolies. According to the U.S. Department of State's *International Narcotics Control Strategy Report*, the increasing concentrations of wealth among organized criminal groups is a concern to legitimate commerce, government, and the integrity of the political process in several parts of the world. Illicit funds and corrupt officials represent a continuing threat to democracy worldwide.

Smuggling currency out of the country in export cargo is facilitated by the freight container itself, which offers considerable opportunities for smuggling bulk currency concealed in legitimate shipments. To illustrate, $18 million of U.S. currency in $20-denominations consists of 900,000 bills, weighing 2,000 pounds and amounting to approximately 40 cubic feet in volume (one measurement ton). The interior space of a standard twenty-foot freight container measures 1,100 cubic feet, which can accommodate 27.5 measurement tons. The practical cooperation of the maritime industry is essential to deterring the opportunities for exploitation of the foreign commercial trade sector by currency smugglers and money launderers.

Future Challenges

Technology and Innovation

All port administrations should identify the requirements for technological equipment necessary to improve security and control access to their port. They must also develop innovative solutions to transport security problems as the criminal element may use new technologies in their criminal efforts. An example may be the development of a satellite communications infrastructure that would be shared with port security systems for the purpose of tracking and securing cargo in transit or at rest. This same technology could be used by criminals to send false signals as to the security of the container, or possibly to redirect the cargo. It is evident that the increasing use of electronic data interchange in the shipping cycle presents information security challenges to port security departments and to the entire maritime transportation industry.

Intelligence Data Bases. In November 1994, the United Nations World Ministerial Conference on Organized Transnational Crime drafted conclusions and recommendations for international cooperation. It was regarded as essential that law enforcement agencies be equipped with software for data bases to be used for tactical and strategic intelligence.

Electronic Data Interchange (EDI). EDI is increasingly used in modern marine terminals. It enables shipping transactions to be conducted entirely from a computer terminal linked to a data network. Transactions include booking freight, tracking shipments, billing customers, and clearing customs.

A modern marine terminal container operation is dependent upon a central computer data base to track arrivals and departures between the vessel and the port gate and throughout the container storage and handling areas. At each transaction in the cycle,

specific details identifying each container are entered into or generated by the computer data base, electronically and in hard copy. The information includes the container's current location and ultimate destination.

Also extracted during that process is information from the ocean bill of lading, which is available on the export load's dock receipt. The ocean bill of lading contains a description of the cargo (e.g., "...packages said to contain..."), and serves as a collection document enabling a foreign buyer to receive a shipment from the carrier by simply showing proof of identity. EDI is, therefore, a potentially rich source of shipping information to cargo thieves and other criminals and must be adequately protected.

Satellite Tracking of Cargo. The integration of data communications and satellite technologies shows considerable promise in the near future for tracking containers, trailers, and chassis. The port security application of this technology is toward combating, for example, hijacking and theft of intermodal containerized cargoes while at sea or during inland transit. Other security applications, other than those related to cargo theft, are also feasible.

Although the responsibility for in-transit tracking of cargo rests primarily with the transporters of the cargo on behalf of its owners, future business arrangements and insurance requirements may necessitate a larger service involvement by port security beyond the physical facility. Security personnel should at least be familiar with the technology, understand its application and be knowledgeable of the trades in which it is used, what companies employ the technology, and what governmental authorities are involved in its application.

The technology could also serve as an accurate and reliable electronic bonding system for the movement of international containerized cargo through customs inspection. In that capacity, customs at the point of export would certify the integrity of the container's seal until it was uneventfully received by customs at the point of import.

One result would be expediting cargo handling at ports of entry by reducing container processing time clearing customs.

Privatization

Seaport privatization plans, which may grant long term concessions to non-governmental organizations to operate ports, have increased productivity, in some cases. Ship turnaround and cargo handling times have been reduced. New competition created among private terminal operators has led to decreased port fees and increased supply and quality of service. A port's security, however, is not necessarily improved as a natural consequence of privatization. It is important that a strong port security program be maintained. In some cases, port privatization has included a relaxation of controls and fewer cargo inspections. These acts have made it easier to smuggle illicit cargoes from those ports concealed in legitimate commercial shipments.

Port Congestion

Port security must be prepared to deal with the maritime crime problems resulting from cargo congestion in ports. In many countries, rapid growth and surges in containerized maritime trade are resulting in severe congestion in marine terminals. Consequently, this is causing inefficiencies in the processing and control of containers, accompanied by expedited customs inspections.

Ironically, a common government response to port congestion is to relax customs inspections in an attempt to expeditiously clear backlogged cargo. These

circumstances create additional opportunities for unauthorized access to idle or misplaced cargo and inspire cursory examinations of shipping documentation. These conditions are providing smugglers with substantial opportunities at relatively low risk.

International Cooperation

A more vigorous international approach is needed to curtail maritime criminal activities. For example, criminal penalties for smuggling aliens are often weak, and smuggling is not considered a crime in many countries. The U.S. Department of State has stressed the importance of multilateral cooperation among governments. Building networks of diplomacy and law enforcement are necessary in order to alleviate such problems as alien smuggling, characterized as not only an immigration problem but also a national security problem.

In addition to working in the international arena to solve port security problems, there is a need to adhere to the conclusions and recommendations of the international organizations capable of providing conscientious assistance to the maritime industry. The Group of Seven Nations/P-8 Senior Experts Group on Transnational Organized Crime conducted a review of existing international agreements, arrangements, and practices to counter transnational organized crime. Their report identified gaps and made recommendations to fill such gaps. General conclusions included that:

> (a) all States should sustain their participation in international organizations to promote cooperation against transnational organized crime, including the United Nations, Interpol (International Criminal Police Organization), and the World Customs Organization;

(b) all States must work closely to share information and expertise; and

© all States should increase their operational cooperation among police forces, customs, immigration, and other relevant agencies.

Conclusion

The increasingly complex nature and international scope of the maritime security issues which threaten the industry requires a wide range of participation and response from all levels of government and the maritime industry. While some ports are comparatively unencumbered by crime, many others are besieged by a wide range of serious problems which threaten the safe and efficient conduct of trade in those ports. The lack of a secure trade corridor can hamper the economic growth of that port and possibly the country itself.

A viable maritime security program is good business. Losses from cargo thefts are estimated to be in the billions of dollars in the United States alone. While the implementation of a security program will entail the expenditure of funds, that expenditure can be more than offset by the savings security can provide. The cost to a port of losing a shipping company's business because of inadequate port security must be considered. We must begin to think beyond the short-term cost and look at the long term benefits such as increased cargo operations which lead to increased port revenues. The potential to reduce local crime is enhanced as more of the surrounding populace finds employment and benefits from legitimate businesses. We must begin to look beyond the simple view that a lack of security affects only the ship and the terminal it calls upon. A much bigger economic interdependency exists within the entire transportation network. Ports must be committed to developing effective maritime security programs based on the recognition of ports as intermodal interchange hubs of commerce, critical to international trade.

Recommended Readings

"Appropriate Modalities and Guidelines For the Prevention and Control of Organized Transnational Crime At the Regional and International Levels", United Nations World Ministerial Conference on Organized Transnational Crime, Naples, Italy, 21-23 Nov 1994 [excerpt in *Trends in Organized Crime*, Vol. 1, No. 2, Winter 1995].

Drug Trafficking and Drug Abuse: Guidelines For Owners and Masters On Prevention, Detection and Recognition, International Chamber of Shipping; 1994.

"The Feasibility of Elaborating International Instruments, Including Conventions, Against Organized Transnational Crime", United Nations World Ministerial Conference on Organized Transnational Crime, Naples, Italy, 21-23 Nov 1994 [excerpt in *Trends in Organized Crime*, Vol. 1, No. 2, Winter 1995].

Fight Against Transnational Organized Crime - Chairman's Statement, Report of the G-7/P-8 Senior Experts Group on Transnational Organized Crime, Paris, 12 Apr 1996.

Financial Investigations: A Financial Approach to Detecting and Resolving Crimes, (Publication 1714), Assistant Commissioner for Criminal Investigation, Internal Revenue Service, U.S. Department of the Treasury; 1993.

"Global Organized Crime: Threats To U.S. and International Security", Global Organized Crime: The New Evil Empire, Conference Proceedings, Center for Strategic and International Studies, 26 Sep 1994; J. Woolsey.

Guidelines On Co-Operation Between Customs Administrations and Port Aimed At the Prevention of Drug Smuggling, Customs Co-Operation Council, prepared for the International Association of Ports and Harbors; Nov 1989.

International Narcotics Control Strategy Report, Bureau for International Narcotics and Law Enforcement Affairs, U.S. Department of State, Mar 1996.

International Perspectives on Maritime Security, Maritime Security Council et al., 1996; [Ed.] T. Fitzhugh III.

Law of the Sea: Report of the Secretary-General, United Nations General Assembly Fiftieth Session, 1 Nov 1995, agenda item 39 (A/50/713); report on developments pertaining to the implementation of the UN Convention on the Law of the Sea.

Legal Aspects of International Terrorism, Evans Murphy, Lexington Books; 1978.

Maritime Security, Cornell Maritime Press, 1989; K.G. Hawkes.

Maritime Security Manual-Part I, American Society For Industrial Security, 1990; [Ed.] H. Gomez.

Maritime Security Manual-Part II, American Society For Industrial Security, 1994; [Ed.] H. Gomez.

Ports At Risk, International Maritime Bureau, 1993; E. Ellen [Editor].

Port Risk Management Guidebook: A Risk Management and Insurance Reference for U.S. Ports, U.S. Maritime Administration; 1985.

Proceedings of the First Inter-American Course On Port Security,

21 Oct-10 Nov 1995, Maritime Security Institute for the Americas, Port of Miami and the Organization of American States Permanent Technical Committee on Ports.

Sea Carrier Security Manual, Pub. No. 546, Office of International Affairs, U.S. Customs Service; Apr 1989.

Standards for Marine Cargo Security, American Association of Port Authorities; 1980.