Appendix D

Technologies To Protect Harbors, Ports, and Vessels

Introduction

A long list of obvious targets of potential interest to terrorists exists at the interface where land meets water. Shipping (especially cruise ships and ships with dangerous or expensive cargo), ferries, dikes, dams, levees, pipelines, oil platforms, cooling water intake ducts, canals, locks, ship yards, crowded beaches, coral reefs, oyster shoals, and other centers of ecological or economic value come immediately to mind. A more careful consideration, in addition, would highlight the importance of maritime industries to national priorities and their consequent attractiveness to terrorists. The importance of maritime trade is reflected in the fact that a very large proportion of the world's trade (by bulk) is carried by ships. In addition, millions of passengers board cruise ships every year.

Yet most Americans, if they contemplate the threat of terrorism at all, do not associate it with ports and harbors. Airplanes, embassies, and military facilities overshadow other targets in the minds of the American public.

Actually, attacks against shipping or other maritime targets are far from rare. Exact figures are hard to come by due to problems with data collection (many acts go unreported) and diverging definitions (e.g., terrorism v. piracy). But according to the International Maritime Organization, 179 known cases of piracy against merchant ships occurred between 1982 and 1989. Other sources claim that as many as 1,000 attacks have taken place from 1979 to 1989.[1] Some of these have been quite spectacular. In 1988,9 people were killed and another 46 were injured during a terrorist shooting spree aboard the Greek vessel City *of Poros. In* **May 1990, Libyan-based terrorists belonging to the Palestine Liberation Front of Abu'1 Abbas swarmed down in speed boats upon vacation beaches in Israel with the intention of directly attacking civilians along the Tel Aviv waterfront. Their mission was foiled by a rapid response by Israeli Naval, Air, and Land Forces, but only by the slimmest of margins.**

Despite their number, only a few of these attacks have won much notoriety within the United States, probably because few directly involved U.S. citizens either as victims or perpetrators. About the only exception is the 1985 attack on the Italian-flag cruise ship *Achille Lauro* (also organized by Abu'1 Abbas), in which **American Leon** Klinghoffer **was** killed.[2] The *Achille Lauro* affair touched off **a** lot of uproar including congressional hearings and court **actions that continue to this day.**[3] But the public **interest accorded this event is much more the** exception **than the rule.**

It is impossible **to determine with** precision why **there have not** been **more and costlier incidents involving our maritime industries. It is likely that something more than luck is involved. Insofar as the hijacking of transportation targets is concerned, several reasons for ruling out ships in favor (from the terrorists' perspective) of airplanes can be pretty easily formulated. For example, in the words of one analyst:**

> **. . .Terrorist and nonterrorist hijackings have plummeted in recent years . . . Takeovers of nonaerial means of transportation (buses, trains, and ships) have not risen to fill the operational void created by the decline in aerial attacks. [Byway of explanation:] Threatening to force the plane into a power dive credibly jeopardizes the lives of more individuals than does any comparable threat against other modes of transportation. Moreover, it is simpler to control the actions of a large number of people on board a plane in flight than it would be to prevent the escape of passengers from a ship.[4]**

Another points out:

> **Whether on the ground or in the air, an aircraft is more fragile than a ship by far, and the density of its cargo, passenger or freight, is high. It boasts of mobility on the order of forty times that of a ship, an important consideration in the hijacker's calculations of his chances for success. What is more, while high-value freight tends to be transported by air, more bulky, low-value commodities go by ship. The conclusion is easy to reach that ships are poor targets for hijacking compared to aircraft. Still, if a terrorist is seeking publicity as his primary objective, the uniqueness of a ship hijacking might have great appeal.[5]**

While some of the above arguments might explain why ships have been relatively immune to the threat of hijacking, it fails to explain why the American maritime

---

[1] M. Wisenhut, "Piracy and the Threat to USTRANSCOM," *Defense Transportation Journal*, vol. 46, No. 4, August 1990, pp. 16-18.

[2] For a good narrative account of this event see Scott C. Truver, "Maritime Terrorism, 1985,' *United States Naval Institute Proceedings, vol. 112, May 1986, pp. 160-173.*

[3] A court recently decided that the *daughters* of Mr. Klinghoffer were entitled to sue the PLO for damages resulting from the incident.

[4] Edward F. Mickolus, *Transnational Terrorism: A Chronology of Events, 1968-1979* (Westport, CT: *Greenwood press,* 1980), p. xxiv.

[5] R.W. Barnett, ' 'The U.S. Navy's Role in Countering Maritime Terrorism, " *Terrorism: An International Journal,* vol. 6, No. 3, 1983, pp. 469-480, at 472-473.

industry has been spared other forms of terrorism, for example: mass murder; or the destruction or the threat of destruction of other marine structures with concomitant economic and ecological damage; or ransom, for example of a multimillion-dollar vessel or an off-shore oil platform.

Few port authorities are so optimistic as to think that ''It hasn't happened here' can be reliably extrapolated to "It can't happen here." But even fewer sense any immediate need to reallocate perpetually limited funds from immediate, pressing issues to address what is currently a theoretical problem. However, as airlines toughen their security measures, as military and government facilities become better defended, as businesses abroad become more astute in providing security, as piracy and smuggling become a means to replace money formerly provided by East Bloc state sponsorship, as temptingly colossal new targets in the form of huge 5,000-passenger liners make their advent, and as the criticality of shipping to the support of our troops abroad (especially in the Middle East) becomes more apparent,[6] it is more than likely that terrorists will turn to untraditional, less hardened targets including ports, harbors and ships.

In addition to apathy, there are other impediments to the orderly implementation of further security measures around ports, harbors, and ships. One of these is confusion over responsibilities. As with any environment as complicated as a port, diverse authorities have hands in many facets of operations, including security. Should an incident occur, any one or several of a bewildering array of frequently overlapping and conflicting authorities could be involved, depending on the nature of the act and the location in which it takes place. Private security companies; port, municipal, local, State, and Federal law enforcement agencies; the U.S. Coast Guard; the U.S. Navy; the U.S. Customs Service; the Immigration and Naturalization Service; the Drug Enforcement Agency; port owners and operators; and the master and owner of each vessel all bear some measure of responsibility for security. Complicating matters, the rivers, lakes, and other bodies of water associated with ports and harbors frequently are used to define municipal, state, or even international boundaries. Therefore, it is not unusual to have to double or triple this already unwieldy list depending on the number of governments involved. And many other entities, including insurance companies, shipping companies, even passengers, unions, and the workers and crewmen they represent, clearly have a stake in a port's security arrangements.[7]

This problem is well recognized and some efforts are now being made to assign security duties unambiguously.

Legislatively, the Coast Guard bears primacy in the area of domestic port and harbor security. However, it is the FBI which is recognized as having primary responsibility for responding to terrorist incidents within the territory of the United States. In order to avoid confusion, these two agencies have signed a memorandum of understanding clearly designating the FBI as lead agency in the event of a domestic terrorist incident. A similar arrangement exists with the Department of State for response to terrorist incidents outside the United States. In the event of an incident, the Coast Guard would follow the direction of the lead agency and supply vessel, air and communication support, trained boarding personnel, and specialized expertise concerning maritime operations.[8] Another group, the National Port Readiness Steering Group, composed of representatives of the Maritime Administration (MARAD), the Coast Guard, the Military Sealift Command (MSC), the Navy Control of Shipping Organization (NCSORG), the Military Traffic Management Command (MTMC), the U.S. Army Corps of Engineers (USACE) and the commands of the Maritime Defense Zones (MDZ), is preparing a study, due out soon, with the goal of ensuring that in the event of a national emergency, the ports and harbors will be up to the task of mobilization. This study will result in a memorandum of understanding among the group members clearly assigning duties including security responsibilities. The group is also a conduit for the exchange of information and communication among its members.

But much confusion still exists among the many other players who face the myriad possible situations and disasters imaginable along the waterfront or on board a ship.

Many questions still remain. For example, while the Magnuson Act and subsequent legislation place ultimate responsibility with the U.S. Coast Guard, implementing regulations (33 CFR 6 et seq.) imply a somewhat shifted burden:

> Nothing contained in this part shall be construed as relieving the masters, owners, operators, and agents of vessels or other waterfront facilities from their primary responsibility for the protection of such vessels or waterfront facilities.[9]

Even in the absence of a coherent chain of command, some security measures are already in existence, although the main thrust of these measures is towards deterring and

[6] See H.W. Stephens, "Port Readiness for Military Mobilization" *Naval Forces,* vol. 9, No. 5, 1988, pp. 14-15.

[7] For more information see Hugh W. Stephens, "Barriers to Port Security, " *Journal of Security Administration, vol. 12, No. 2, 1989,* pp. 29-41.

[8] Admiral Joel D. Sipes, "Maritime Terrorism, " *Proceedings of the Joint Government-Industry Symposium on Transportation Security,* Williamsburg, VA, Mar. 21-22, 1990.

[9] 33 CFR 6.19-1.

responding to conventional criminal activities such as theft and smuggling. And there are several efforts under way to assess waterfront security needs and develop new equipment to meet them. As has been shown in our earlier report,[10] the first and best line of defense against any criminal or terrorist security threat lies not with technology nor with new machinery. Rather, there is clearly no substitute for vigilant, well-trained human beings alert to and reporting on suspicious activity. Still, to the extent that technology can assist these efforts, it should be supported. This appendix will describe technologies currently in use, on the drawing board, and just being envisioned for helping to ensure the safety of people and equipment in and around ports and ships.

U.S. Coast Guard Activities and Other U.S. Government Measures Against Terrorism

Any good security system, wherever located, must be capable of providing several functions, including prevention, detection, assessment, denial, delay, and response. In many instances, the equipment and procedures for providing these capabilities for land-based facilities are equally applicable to the marine environment. This is not particularly surprising since the two frequently face the same challenges: intrusion prevention and detection, contraband detection, access control, identity verification, site hardening, and so on. Many of these technologies are dealt with in appendix E and will not be further treated here except insofar as measures unique to the maritime environment are concerned.

However, one significant feature differentiates ports, harbors, ships, and other maritime structures from dry land: the presence of water. Water allows means of intrusion that find no parallel in considerations of shore security including swimmers, divers, fast surface boats, subsurface vessels (e.g., minisubs), and floating debris. This section will present some of the actions currently being taken and some of the technologies currently in place to combat the threat of terrorism in this environment.

Historically, the Coast Guard has borne the primary burden for domestic port and harbor security starting with enactment of the Espionage Act of 1917, although at the time this act was considered to apply only under wartime conditions.[11] In addition to its well-known inspection, with patrol, and safety functions, the Coast Guard administers several measures for improving port security by controlling access to port facilities, preparing contingency plans, and training personnel, which will be described below.

One of the most effective ways to prevent an incident is to block access to a vulnerable area. In addition to the obvious expedients of fences and locks, some means must be applied to permit entrance of authorized individuals while denying it to others. One of the current methods centers around the U.S. Coast Guard Port Security Card.

In 1950, President Truman signed Executive Order No. 10173 (later amended by Executive Orders Nos. 10277, 10352, and 11249) prescribing the creation of regulations "relating to the safeguarding against destruction, loss, or injury from sabotage or other subversive acts, accidents or other causes of similar nature, of vessels, harbors, ports, and waterfront facilities. ' This led to Part 6, Subchapter A, Chapter I, Title 33 of the Code of Federal Regulations: Protection and Security of Vessels, Harbors, and Waterfront Facilities.[12]

The only significant security measure engendered by these regulations was the requirement for persons seeking access to certain port facilities at certain times to possess an acceptable identification credential, most commonly a U.S. Coast Guard Port Security Card. This is a traditional picture ID with a signature and descriptive data. The card and surrounding procedures have been little changed over the 40 years of their existence and are now clearly antiquated. An applicant fills out a form and undergoes a background check. Problems with the card system include ease of forgery, relatively low durability, and, perhaps most importantly, lack of flexibility. Early court challenges established that wholesale denial of access to the general dock area by noncard holders was improper because such a procedure arbitrarily cuts off a worker from his livelihood. Therefore, the card system is now used (for official access control) only in areas of designated national security interest or under conditions of documented threat.

Controlling access to port facilities from the waterside is also a necessity although it is a little trickier. Insofar as overt waterside entrance is concerned, the Coast Guard has implemented various rules and regulations concerning entry into U.S. ports by foreign shipping, especially from what used to be known as the Eastern Bloc. However, terrorists, who have little interest in a long-term commercial relationship with their victims, would belittle inclined to advertise their arrival by voluntary compliance with these regulations. Still, to the extent that many terrorist groups operate out of known geographical areas and are likely to travel from these areas, these regulations do permit some control over the arrival of high-risk individuals. Routine controls by the U.S. Customs

[10] U.S. Congress, Office of Technology Assessment, *Technology Against Terrorism: The Federal Effort,* OTA-ISC-481 (Washington, DC: U.S. Government Printing Office, July 1991).

[11] This limitation was lifted in 1950 when the Magnuson Act (50 U.S.C. 191) amended the earlier legislation and madeport security a permanent Coast Guard duty. The Ports and Waterways Security Act (codified as 33 U.S.C. 1221-1227), passed in 1972, further broadened the Coast Guard's authority to take actions regarding security and provided some mechanisms for doing so.

[12] See also 33 CFR 125 et seq.

Service and the Immigration and Naturalization Service at all ports of entry help to deter and detect terrorist efforts to enter U.S. ports overtly from overseas. The Coast Guard is also involved in other counterterrorist efforts, primarily of an assessment and planning nature (see next section).

Role of the International Maritime Organization

In the aftermath of *the Achille Lauro* hijacking in 1985, the International Maritime Organization (IMO), which operates under the aegis of the United Nations, drafted proposed guidelines for security for passenger vessels and the facilities that service them (IMO Circular 443, published 1986). This proposal was largely the product of the United States' representatives (specifically, the U.S. Coast Guard and State Department) to the IMO. While the guidelines present a useful framework for assessing port security needs and implementing appropriate measures, they are strictly voluntary. The degree of compliance with the measures, both national and international, varies considerably from port to port but, while progress is slowly being made, concrete changes have generally been modest.[13]

The IMO measures were acknowledged and enlarged upon in the Omnibus Diplomatic Security and Antiterrorism Act of 1986, Title IX of which relates to International Maritime and Port Security .14 This law in part amended the Ports and Waterways Security Act, encouraged the President to continue to seek improved international seaport and shipboard security and suggested several measures to help reach that goal. The law also mandated that the Secretaries of Transportation and State produce various annual studies and reports on the topics of maritime terrorist threats and security at foreign ports. If the situation in a foreign port were found to be serious enough, and no remedial action were taken, issuance of a travel advisory was authorized. To date, no such advisory has been found necessary.

Congressional support for these measures has been minimal. For example, of the $12.5 million annual expenditure authorized by the bill, only $903,000 was appropriated in the first year.[15]

In large measure, implementation of the law fell to the Coast Guard. The text accompanying publication of the IMO Circular in the Federal Register[16] made clear that the Coast Guard intended to avoid across-the-board requirements, opting instead for a ship-by-ship and port-by-port appraisal and voluntary compliance. Other Coast Guard actions in support of the IMO Circular and the law included the creation and support of local Port Readiness Committees as a forum for coordination among the participating agencies concerned with the issues of port security especially where support of a military mobilization is concerned. The Department of Transportation is planning to issue regulations shortly for implementing IMO guidelines in the United States. In his 1989 report to Congress, the Secretary of Transportation noted that over 80 percent of the ports surveyed had established a Port Readiness Committee and over 50 percent of these included a Security Subcommittee.

The Coast Guard has also developed or supported several training programs designed to improve security awareness and capabilities for both domestic and international (under the Antiterrorism Assistance Program of the State Department) port authorities:

- Port Security Committees.
- Port Readiness Committees. The primary purpose of a Port Readiness Committee (PRC) is to "foster communication, cooperation and coordination among member agencies to strengthen the capability of commercial seaports to support deployment of military personnel and cargo in the event of mobilization or national defense contingencies."[17]
- Maritime Counterterrorism Contingency Plans.[18]
- USCG Training Programs.
- U.S. Training Programs for the Maritime Industry.
- U.S. Port Security Assessments.
- Foreign Port Security Assessments.

While these measures are laudable insofar as they go, they have been criticized as being too lenient and misdirected.

> . . . [T]o the degree Title IX and Coast Guard actions go beyond recommendations, the focus is upon inspections, training, and lighting, fences and other means to discourage casual entry. In their aggregate, these efforts suggest that government and industry have concluded that physical barriers and supporting practices designed to limit physical access to ports and ships are sufficient protection against plausible

[13] See "A Report to Congress on Passenger Vessel and Port Security, ' prepared by the U.S. Department of Transportation in compliance with Title IX of U.S. Public Law 99-399. This report evaluates national and international port and harbor security and is prepared yearly by the DOT as part of the United States' implementation of the IMO guidelines.

[14] 46 U.S.C. app. 1801 et seq. and 33 U.S.C. 1226.

[15] Stephens, op. cit., footnote 6, 1989.

[16] 52 *Federal Register*, 11,587-11,594 (1987).

[17] For more See A *Report to Congress on Passenger Vessel and Port Security* prepared by the U.S. DOT in compliance with Title IX of Public Law 99-399, Feb. 28, 1989.

[18] Ibid.

terrorist threats. Indeed, these may help to frustrate the isolated terrorist strike. But well-armed and trained terrorists or enemy special operations units bent on wreaking destruction and casualties will certainly not be deterred and scarcely inconvenienced by such measures.[19]

The Coast Guard is making some efforts to develop new responses to the threat of terrorism. Some of these will be described in the next section. However, in the absence of clear national priority or documented terrorist threats, it is unlikely that the Coast Guard will be allotted the resources to design and develop more exotic countermeasures.

In countering terrorism, forewarned is forearmed. Another service of the U.S. and other governments involves making sure mariners have up-to-the-minute information on factors affecting their safety. For some time now, it has been governmental practice to provide mariners with information affecting the safety of the shipping lanes including severe weather alerts, shipping lane blockages, and buoy or lighthouse changes. The Defense Mapping Agency is responsible for collecting and disseminating such Notice to Mariners. To do so, they have developed an Automated Notice to Mariners System (ANMS) containing information dealing with navigational safety. This system is part of DMA's Worldwide Radio Navigational Warning Broadcast System. Mariners around the world can connect to the system via satellite, telephone, radio, or computer hookup and access current information on a variety of topics. They can also file reports to be added to the database. In the early 1980's, the need for information about piracy and other attacks against shipping was recognized. Not only were these data of obvious interest to the mariners venturing into high-activity areas, but the governmental bodies charged with countering the threat of maritime terrorism had been hampered by the lack of accurate, comprehensive data on the magnitude of the problem. The U.S. Interagency Working Group on Piracy and Maritime Terrorism asked the DMA to expand its NAVINFONET system to include such warnings. With a few software changes, DMA complied with the creation of an automated message subsystem: the Anti-Shipping Activities Message File or ASAM of the Broadcast Warning System. Generally speaking, the incidents reported on this service are gathered from open sources such as newspaper accounts. Warnings and reports filed by mariners themselves are not checked for accuracy and NAVINFONET accepts no legal liability for the accuracy of the information. The purpose of the service is **to** provide warnings and this **mandate can be fulfilled even with slightly faulty data.**

There have also been initiatives from the private sector to beef up security. These are motivated not only by humanitarian concerns about risks to the lives and limbs of passengers and employees, and financial concerns about loss of property, but also by a rising consciousness of possible legal liability and insurance problems arising from failure to take reasonable precautions in today's hostile world.

> **Legal liabilities for negligent security practices are increasing and, as a result, the need for better maritime security is increasing. During the lo-year Persian Gulf War over 500 crewmembers aboard commercial vessels were either killed or wounded. These casualties have spawned all sorts of litigation, particularly in the United States, and one of the issues raised in these lawsuits is the seaworthiness of the vessels themselves. Insurance coverage very often depends upon the seaworthiness of the vessel insured at the time her voyage begins, and if it can be shown that a particular vessel was not seaworthy (that is, not fit for her intended use) because she was inadequately prepared for the security threats she faced, a precedent may be established which the maritime industry cannot afford to ignore. . . Shipowners, offshore installation operators, and port authorities are going to be held accountable in the future when their negligent security practices allow a terrorist incident to occur.**[20]

These security efforts have been primarily directed at **access control and baggage screening.**

About 3.2 million cruise-line passengers pass through the Port of Miami every year[21] **making it the largest cruise-line port in the United States. (Miami alone handles about one-third of all scheduled departures of major cruise ships from U.S. ports.**[22]**) At all the passenger terminals, the private cruise lines have provided x-ray and metal-detection equipment for screening all passengers and their carry-on luggage, much the way airlines do today. These units are not particularly expensive, as security equipment goes, about $120,000 per portal. But Miami alone needs about 12 of them to cope with its passenger flow. Furthermore, there are two gaping shortcomings in this scheme. First, there is no screening of checked baggage. Not only does this allow the emplacement of time bombs and other remotely operated devices but, unlike their airline counterparts, cruise**

[19]Stephens, *op.* cit., footnote 6, pp. 31-32.

[20]From ''Mva[e Security Services and the Maritime Industry,' a speech by Kenneth Gale Hawkes, Vice President, Maritime Security, Wackenhut Services, Inc., 1990.

[21]Captain Herman Gomez, Director, Training, Plarming & Development Seaport Authority, Port of Miami, personal communication, Oct. 11,1990.

[22]According t. the *Official Steamship Guide* as quoted in report on the hearing held Oct. 23, 1985 before the House Committee on Foreign Affairs on Overview of International Maritime Security.

passengers have access to their checked baggage, which is placed in their cabins before departure. Anyone who wanted to bring firearms aboard ship would not find it difficult. A second big problem is that passengers routinely disembark and reboard at ports throughout the cruise itinerary. Frequently these ports are either too small or too poor to offer much in the way of security services. Again, there would be little impediment to the smuggling of weapons or undesirable individuals on board by even the least resourceful of terrorists. Still, these measures by the Port of Miami are an important beginning.

One cruise line, Royal Viking, is taking matters into its own hands. It is arranging to equip its vessels with a portable security office: a small container furnished with x-ray and metal-detection equipment. The container is carried on board to be deployed when necessary. Returning passengers would pass through it as they reboarded.[23] Some cruise-line organizations are now considering bringing pressure to bear against ports in particularly risky areas by threatening to exclude such ports from their itinerary unless security is improved.

There are some problems with applying even these tried-and-true technological measures to port security. The environment around ports, harbors, and marine structures is particularly harsh: high humidity, salt water, motion, and storms are factors that find no parallel in the typical airport scenario. Therefore, it is not surprising that equipment for cargo and passenger inspection cannot be simply transferred from one mode to the other. Still, the concepts of x-ray and metal detection are viable although the implementation must be more rugged.

Insofar as self defense is concerned, civilian shipping generally employs few technological novelties. Many mariners are reluctant to bear weapons. They would rather not engage in literal combat with terrorists and pirates, seeing this as a task for the Coast Guard or Armed Forces who are better trained and better equipped for such activities. Generally speaking, this is the same approach recommended by the U.S. Department of Transportation's Maritime Administration whose position on the subject can be summed up in the title of its small brochure, *Piracy Countermeasures: Anticipate Trouble, Be Vigilant, Don't Be Heroic. The* measures suggested by this brochure are commonsense precautions such as posting guards, keeping unauthorized personnel off the ship, and making sure that the ship and surrounding areas are well lit. If pirates actually board, crewmen are advised to barricade themselves and any critical areas of the ship (e.g., the bridge) and radio for help. The most aggressive measure suggested by this brochure is the use of searchlights to dazzle suspected hostile boarding parties.

Some industry activists would like to see a little less passivity. A small but growing maritime security industry is specializing in assessing the vulnerabilities of port facilities and ships themselves and providing recommendations on measures to discourage criminal and terrorist activity. For example, Wackenhut, a corporation long involved with land-based security systems, recently started anew division devoted to maritime security. These recommendations include measures up to and including what sort of force to apply to repel unwanted boarders. High-pressure water hoses are a favorite.

Proposed Security Systems and Their Costs

U.S. Coast Guard Entry Cards

As previously noted, several deficiencies exist in the Coast Guard's antiquated identity card system. The Coast Guard is now in the process of developing and procuring a replacement for the current system to be known as the Port Access Control System (or PACS). This system will involve anew, more rugged and tamper-resistant identification card and a computerized local database. The card will not contain any visible identifying information but will be imprinted with a hidden computer readable bar code. At the time an individual applies for the card, a video image of the applicant will be made and stored on the database along with other biometric and identifying information. The cards will ordinarily be stored at the office of the local Captain of the Port. However, in times of emergency, they will be distributed to the port workers. In order to gain access to a controlled access area, a port worker would have to enter through a manned checkpoint equipped with a card reader. On inserting the card into the reader, a picture of the worker's face and other data appear on a television monitor where the guard can verify identity. By making use of computer technology, a system much more flexible than the current Port Security Card is possible. Access rights could be tailored to each individual's duties. Updating of information would be possible without having to reissue cards. Finally, tapes could be exchanged nationwide so that individuals found to be suspect in one area of the country could be quickly barred from ports in other areas. A prototype system has recently performed satisfactorily during testing and evaluation in New Orleans and is slated for further testing this year. Based on cost figures for the prototype, the Coast Guard estimates that each PACS will cost about $33,000. No finds are designated for this project in fiscal year 1991. A budget funding request for $2 million in fiscal year 1992 has been submitted for procurement and national distribution of the PACS to USCG field units.

USCG Underwater Sensing System

Another USCG innovation is the Surface Contact and Underwater Tracker or SCOUT, a multiple sensor system for detecting, locating, and identifying waterborne or submerged intruders. SCOUT is being developed jointly

[23] Norm Miller, ScanTech Corp., NJ, personal communication Oct. 10, 1990.

with the Naval Sea Systems Command. The novelty in this system lies **not with its instruments** and **sensors** that are **all conventional (sonar, radar, low-light closed-circuit TV), but the fact that they are integrated and carried on a mobile platform, specifically a van. This allows coverage of a large geographical area with only a few units. SCOUT is expected to be deployable by the end of fiscal year 1992. An enhanced workstation for optimizing sensor placement is expected in fiscal year 1993. The frost unit will cost about $2.5 million. Additional units, assuming no major overhauls, would run about $1 to $1.5 million each.**

Underwater Acoustical System

Finding **an** underwater intruder **is a** difficult **task** Human hearing **was** designed **to** operate in air and is less effective when immersed in **water. Sight is limited by water turbidity, particularly in many ports. Regular human patrols of the immediate area are usually not feasible. Therefore, detection of unauthorized swimmers or submersible craft must depend on mechanical surveillance. Several systems for this purpose have been proposed.**

A major problem with controlling access from and through the water is that few means for reasonable escalation of force are currently available, Once detection is accomplished there are few options short of deadly force to deter or stop an intruder.

One corporation, GT-Devices, a subsidiary of General Dynamics, is trying to interest the Navy and other authorities in their system, which, they believe, can stop an intruder without use of deadly force.[24] The Underwater Deterrent Security System is advertised as a nonlethal human-swimmer defense system. It is based on an array of electrothermal sources that would be permanently emplaced underwater. The sources are capable of quickly generating energetic plasmas and thereby producing a high-intensity, directional acoustic emission. The magnitude and direction of the pulses are supposed to be adjustable. The acoustic pulses are generated by the rapid (microsecond time scale) discharge of high energy (on the order of kilojoules) electrical pulses. These cause explosive formation of plasmas in the water and resultant pressure waves. Several plasma generators are organized into a phased array. The company has actually produced a 16-generator array for testing purposes. By controlling the amount of power to each plasma generator, the magnitude and direction of the resulting pressure pulse and the location in which the pressure waves combine to reach maximum intensity may be controlled. At low power, the pressure waves may be used as sonar to detect, track and range. As power and pulse repetition frequency are increased, the effects of the system **increase, going from** unpleasantness **to** pain **to** physical injury. Because **it can be** focused, the manufacturer **asserts that** collateral damage **to** adjoining **structures or** organisms **can be** controlled. The useful range **of operation for the steerable device is up to 1.5 kilometers from the fixed underwater installation, according to GT-Devices. Some** observers are skeptical **of this estimate. The true effective range would have to be determined by testing in open water.**

The system has demonstrated (in the laboratory) an ability to bend metal, indicating that it may also be suitable for deterring intrusion by underwater craft. The system is reported to operate with a 4-kilowatt generator, although the generator size will depend on the desired range. The Navy, for example, is interested in a 600-meter warning zone and a 200-meter keep-out radius. With their test array of 16 emitters, the manufacturer indicates that the system can achieve a focus spot only a couple of meters wide at a range of 200 meters.

Following an initial development contract, the Navy has not been interested in supporting this technology further, making several arguments. First, that it still needs too much money to get to advanced development. This would be inconsistent with the Navy's ''off-the-shelf" philosophy. The Defense Nuclear Agency has shown some interest in the project, but would have to cancel other programs to pay for it. It is said to use too much power in a realistic configuration. Further, its function comes under active denial, which is handled by the Air Force. The focus is at a preselected distance and spot and the beam is very narrow. The Navy asserts that it would need a unit every 100 feet or so.

The Navy Waterside Security System

Following several intrusions in 1984 at the Electric Boat facilities in Groton, CT, where much of the Navy's nuclear powered submarine development work is carried out, the Navy decided that current waterside security capabilities were inadequate. They felt the need to improve their ability to detect, assess, and respond to intrusions by high- and low-speed boats, surface swimmers, scuba divers, and explosives and other inanimate threats hidden in floating debris. In conjunction with the Coast Guard, NASA, the Department of Energy and the Canadian Government, the Navy set about developing an integrated, multi-sensor, automated system, dubbing the project the Waterside Security System. The plan originally envisioned a nearly fully automated and integrated system whereby, for a site the size of the submarine base at Bangor, ME, a single human operator could monitor the waterside security status for the entire installation. The operational requirements of the system were:

[24] See N.K. Winsor and R.B. Ashby, "Underwater Deterrent Security System (UDETSS),'' GTD-90-2, 1990.

Underwater and surface swimmer	Detection to 200 yards @ 0.90 detection probability
Surface craft	Detection to 1,000 yards @ 0.95 detection probability
Operational availability	0.90
False alarm rate (FAR)	1 per 2 hours
FAA (long-term goal)	1 per 8 hours
System cofilguration	Fixed and transportable

The first approach attempted to use off-the-shelf technology as much as possible. This generally turned out to be possible for the sensing systems that consist of sensitive but conventional radar, closed circuit television (both normal and low-light systems), and forward-looking infrared (FLIR) detectors. An exception to this rule was the sonar system, which requires some developmental work. The communications, command, and control (C^3) system has turned out to be more complicated. No off-the-shelf system was capable of providing the automatic targeting and alarm capabilities the Navy felt were critical to successful implementation. With the help of the Canadian government, which has funded about 55 percent of the research and development costs of the C^3 system, the Navy expects to test systems operation in 1991, perform additional testing in 1992, and field operational systems in 1993.

It does little good to know that an intruder is present if there is no way to deter his mission. One problem in the waterside environment is the lack of credible, escalatable countermeasures. Frequently, commanders find that there is little in their arsenal short of deadly force (e.g., dropping hand grenades in the water) with which to respond to a waterborne threat.

The Navy is working to develop several such measures. The first is straightforward: light. Not only is it harder for a intruder to get away with his plan when the targets of his malfeasance are well illuminated, but, the Navy has found, with sufficient power, light itself is capable of delaying, even disorienting, an intruder. For this reason, part of the Waterside Security System consists of a 4-million-candle-power lighting system capable of casting a beam over a mile. Like the other parts of the system, the high-power lights are controllable from the console of the security watchman.

Another response measure on which the Navy relies is marine mammals. The animals can be trained to do many of the actions for which police departments frequently use dogs. They can detect intruders and raise an alarm. They can also be trained to act aggressively towards an intruder. Training and maintaining marine mammals is not easy, however. Unlike dogs, marine mammals are not pack animals and are not motivated by a desire to please the putative pack leader (the trainer). They will work for food but when their hunger is satisfied or when they get tired, they stop. It takes about 2 years to train a dolphin and, of course, there are considerable costs connected with the care of the animal once it is released to service. Still, to date, many Navy security personnel consider patrol by marine mammals one of the most effective measures available.

A comprehensive security system includes delay tactics as well as detection and response components. Toward this end, the Navy is working on development of waterside barriers. A 1985 effort aimed at a barrier capable of stopping a high-speed boat would have cost $2,000 per foot (just for hardware and installation; maintenance was extra). Antiswimmer nets are similarly expensive and invoke a host of environmental problems. The United Kingdom, facing a very real threat from IRA terrorists, has been willing to make large investments in barriers. The Navy would like to be a little more frugal. Still, for a fast boat attack, the Navy recognizes that a barrier is the only defense option. There is no time between detection and disaster to formulate any other response.

Work is now going on to develop a rapidly deployable (on the order of a day), low-cost (on the order of $200 per linear foot) barrier capable of stopping a 50-foot cigarette-type boat approaching at 45 knots. The latest model is down to a promising $500 per linear foot with most of the cost arising from the preparation of permanent mooring fixtures on the bottom. This kinetic barrier, a floating arrangement of PVC piping and wire, has a submerged foil. When struck at high speed, the foil "digs" into the water, causing the barrier, and with it the speed boat, to flip over. Scale models have been tested at California Polytechnic University, San Luis Obispo, and full-scale crash tests are planned shortly at Port Hueneme, CA. This approach has several advantages. Except for the moorings, the system components can be stored in a protected environment. This sheltering from the elements substantially reduces maintenance costs. In the event of a documented threat, the barrier can be installed fairly quickly and on a' 'low-tech' basis. The moorings, on the other hand, even in the absence of the fencing, are useful for clearly defining the security perimeter. Such a clear demarcation is a useful legal tool for specifying what level of action is appropriate at what distance from the facility.