

Commercial Ship Self Defense Against Piracy and Maritime Terrorism

Brian L. White, MTS Member
Vice President, Arion Systems, Inc
15059 Conference Center Drive, Suite 200
Chantilly, Virginia, 20151-3802, USA
bwhite@arionsys.com

Kenneth J. Wydajewski, P.E., MTS Member
Ocean Engineer, Arion Systems, Inc
15059 Conference Center Drive, Suite 200
Chantilly, Virginia 20151-3802, USA
ken.wydajewski@arionsys.com

Abstract—Piracy continues to be a very real problem for ship operators, ship owners, cargo owners, insurance companies, flag states, and host states. Fortunately, the nature and locations of modern day acts of piracy tend to be fairly predictable and are concentrated in certain regions of the world. Potential acts of maritime terrorism are highly unpredictable and pose a worldwide threat since terrorists may attack a country's interests abroad. Commercial ship operators can take concrete steps to help defend themselves against maritime terrorism and piracy. Many ship self defense countermeasures against piracy and maritime terrorism are simple and inexpensive to implement. Developing a thorough ship security plan is essential for commercial ship self defense.

I. INTRODUCTION

Combating piracy and maritime terrorism is certainly a formidable task. The task is multi-lateral in the sense that many groups must actively participate in a cooperative manner to achieve success. The vast spectrum of participants ranges from groups of nations (like the United Nations and various alliances), to individual ships at sea. The middle of the spectrum includes individual governments, military forces, law enforcement organizations, regulatory bodies, trade organizations, insurance carriers, shipping companies, ship operators, etc. This paper focuses on one extreme end of the spectrum and describes what ship owner/operators and ship crews can do to defend themselves against acts of piracy and maritime terrorism.

II. PIRACY

In response to the growing number of worldwide incidents of piracy, the International Chamber of Commerce's International Maritime Bureau (IMB) created the IMB Piracy Reporting Center (PRC) in 1992. The PRC, located in Kuala Lumpur, performs two main services: to issue regular reports on acts of piracy and armed robbery, and to analyze piracy data and issue consolidated reports to interested parties.

A. Piracy Terminology

Terminology is important. The definition of piracy and armed robbery used by the IMB for statistical purposes is "an act of boarding or attempting to board any ship with the intent to commit theft or any other crime and with the intent or capability to use force in the furtherance of that act" [1]. This definition is tremendously broad since the acts need not be successful but only attempted, and what constitutes an attempt is often in the eye of the beholder. Also, this

definition lumps all crimes on vessels together regardless of where they occur. A crime committed on a vessel pierside is just as much an act of piracy as a crime committed on a ship on the high seas by this definition. A host nation would probably view a theft aboard a vessel pierside no differently than any other theft occurring within the port city. The crime of common theft would be handled under the jurisdiction of local and national authorities and would not be considered by them to be piracy. However, if the incident were reported to the PRC, the crime would be considered piracy and included in their reports and statistics.

The International Maritime Organization (IMO) adopted a definition of piracy that included only crimes committed on vessels on the high seas or otherwise outside of the jurisdiction of any state. This definition made sense since the IMO is a multi-national body that is not to meddle in the affairs of individual states. Crimes committed within the borders of a state's jurisdiction are part of the affairs of that state and do not constitute piracy in the IMO's view. The problem is that the majority of attacks occur within the limits of states' jurisdictions. The IMO is considering draft language that distinguishes between piracy and armed robbery against ships. In the draft Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery Against Ships, piracy is defined as follows:

"Definition of Piracy consists of any of the following acts:

- (a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed-
 - i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
 - ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;
- (b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;
- (c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b)" [1].

In the same draft Code of Practice, armed robbery against ships is defined as follows:

“Armed Robbery Against Ships means any unlawful act of violence or detention or any act of depredation, or threat thereof, other than an act of “piracy”, directed against a ship or against persons or property on board such ship, within a State’s jurisdiction over such offences [1].”

The point in discussing these two different definitions is that one must be aware of the subtleties of the definitions and the impact they have on piracy data. For example, both the PRC and IMO definitions exclude acts of fraud without violence. Since the IMB’s PRC is the most widely known and used source of piracy data, the PRC definition and statistics are used in this paper.

B. Piracy Statistics and Trends

Fig. 1 gives the total number of attempted and actual pirate attacks worldwide from 1991 through 2001. In spite of a few ups and downs, the data presented in Fig. 1 demonstrates that the number of attacks has increased since 1994. There is approximately one piracy attack per day and approximately two crew/passenger deaths per month.

In 2001, the number of ship hijackings was double the number in 2000, and the number of cases in which a ship was fired upon increased by 75 percent. Although it is impossible to tell if these alarming statistics are realistic trends or one-year anomalies, authorities are concerned.

There are many possible reasons that may explain why piracy is increasing. One reason is a decreased level of policing of the world’s oceans by the large naval powers of the United States, the United Kingdom, and Russia [2]. The real or perceived level of deterrence is lower now than it was a decade ago. Another big reason for the increase in incidents of piracy is the political instability, economic hardship, and general inability to provide adequate law enforcement in some third world countries. Such a combination of attributes creates an environment ripe for crime, including piracy. These same countries do not have the resources to detect, pursue, or prosecute armed gangs and other crime organizations. In many of these types of areas, piracy and other forms of crime are an illegal but nevertheless accepted form of income. Organized armed gangs are becoming increasingly sophisticated and bold in their pursuits, and there is an overall growth of organized crime. Recent incidents indicate the existence of transnational gangs or organized crime syndicates that cross national boundaries. As far as ships are concerned, vessel masters are facing these disturbing trends with decreasing crew sizes.

One must be prudent when using and interpreting piracy statistics and a few words of caution are noteworthy. As noted earlier, there are many possible definitions of piracy and the one chosen by a particular organization is often related to the organization’s motives. Since the definition of

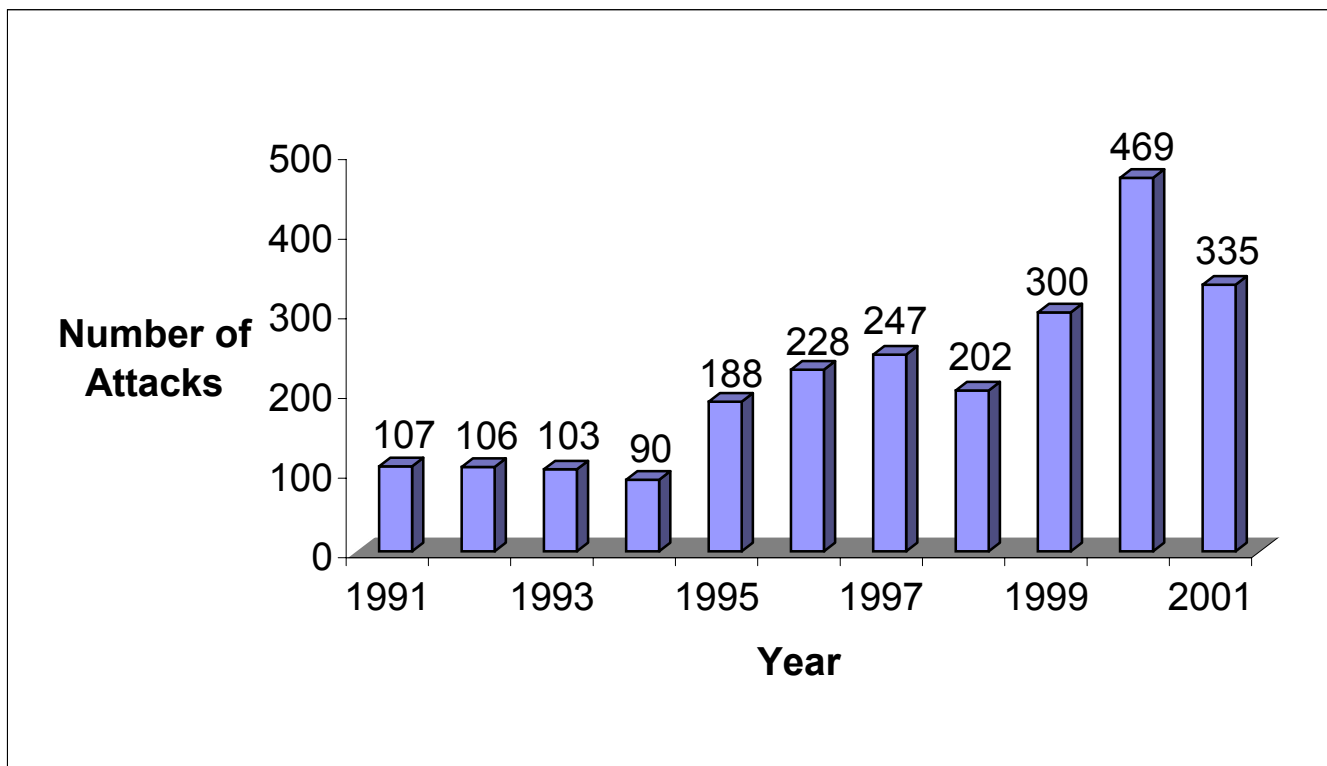


Fig.1. Total number of attempted and actual piracy attacks [source data obtained from Ref. 1]

piracy determines the statistical outcome, one must understand the definition to determine exactly which crimes are included in the tally. Since the IMB is an industry-funded organization, many of which are insurance companies, they adopt a rather broad definition of piracy that results in high numbers of piracy incidents. One can imagine that an insurance company would not be disappointed in high piracy numbers, which could be used to justify their rate structure and special premiums for primary piracy regions. Other organizations, such as a local chamber of commerce or port authority may adopt a much more restrictive definition of piracy to keep the number of incidents to a minimum. Their motive might be to demonstrate the safe and efficient workings of their port in an effort to convince potential customers to use their facilities.

Sometimes a crime is labeled as piracy when another type of crime may have actually been committed. What may appear to be an act of piracy may actually be fraud or even a labor dispute. In a recent incident, a crewmember committed an apparent act of mutiny in international waters by killing the master and mate of a cargo vessel and taking over the ship. The crewmember was eventually overcome by the crew and welded into a stateroom for detention. The preliminary investigation revealed the crewmember's side of the story. He was hired by an agent and told of a large signing bonus in addition to salary. He reported for duty only to find out that the signing bonus went entirely to the agent and was never intended for him. Furthermore, he was not allowed to leave the ship for months in spite of his repeated appeals for leave to go home and visit his family. In his mind he had been kidnapped and was enslaved. He eventually snapped and acted violently. What crime was actually committed and who has jurisdiction? Was it piracy on the high seas? Was it a mutiny that is internal business for the flag state? Was it a labor dispute? Who has jurisdiction in this case? Interestingly enough, the United States claimed jurisdiction because a US vessel responded to the emergency call for help by the vessel's crew on the open ocean. The case is still pending and these questions are still unanswered.

Fraud may be the most common crime that ends up being called piracy. In one possible scenario, the ship owner may find it more profitable to sell the cargo to a black market buyer due to unplanned delays in delivering and discharging the cargo as planned or due to the skyrocketing costs of operating an aging, poorly maintained ship. The vessel owner arranges with a local gang for the ship to be hijacked, the cargo sold, and the vessel and crew to be ransomed. While the cargo insurers pay or litigate with the cargo owner for the total loss of the cargo, the ship and crew are back in business as soon as the small ransom is paid. For the purposes of piracy statistics, the incident is labeled piracy, including a ship hijacking and a crew taken hostage when in actuality the incident was an inside fraud job.

Most knowledgeable persons believe that actual occurrences of real piracy are under-reported. There are

many reasons for under-reporting. Masters are often reluctant to report incidents of piracy for fear of being delayed by investigations and proceedings. Agents, terminals, and port authorities are suspected of being reluctant to take and pass along reports of piracy because of increased workload, bad publicity, and fear of reprisals from the criminals. Authorities may also be reluctant to pursue criminals and to cooperate with other outside authorities for the same reasons. Many acts of piracy do not get reported simply because of geographic distance. Even the weakest attempt at surveillance or boarding in the Straits of Malacca will quickly be reported as piracy to the nearby reporting center in Kuala Lumpur, but the same events in North or South America may never reach the PRC. If the event is not reported directly to the PRC or is not discovered by one of the PRC's operatives, the incident will not become part of the piracy data set.

C. Piracy Generalities

The locations of piracy attacks are shown in Figure 2, in which the stars represent concentrations of attacks. Over two thirds of the world's piracy incidents occur in and around only eight countries or bodies of water: Indonesia, Malaysia, Straits of Malacca, Bangladesh, India, Gulf of Aden and the Red Sea, Nigeria, and the Ivory Coast [1].

Most pirate attacks occur within sight of land. In fact most attacks occur while the ship is at anchor and during hours of darkness. The typical attack starts with the target ship being approached by one or more small craft that vary from primitive, homemade vessels to modern high-speed craft [3]. Ships at anchor will be approached near the bow or stern and a boarding will occur by any of several means including the use of grappling hooks. Ships underway will be approached and boarded alongside or near the stern depending on the freeboard and ease of access in those areas. In general, ships with low freeboard that travel at relatively low speed are prime targets for pirate attack.

According to the IMB, pirate attacks can be divided into three main categories: petty theft, planned robberies, and permanent ship and cargo hijackings. The majority of attacks are in the petty theft category. The goal of most of these pirate attacks is to make a quick score of items that can be easily sold for profit. The most commonly stolen items are mooring lines, cans of paint, food and stores, and crew belongings and money. Planned robberies are much the same as the petty thefts except that well-organized, well-armed gangs often carry out the acts. Ship's equipment is also often stolen in addition to the petty theft items already mentioned. In permanent ship hijackings, the entire ship and its cargo are stolen. The crew, in this case, is either murdered, set adrift, or held hostage for ransom.

The number of ship and cargo hijackings is on the rise. Organized crime with transnational connections is almost always involved and there is sometimes suspicion that corrupt state authorities may be involved or complicit. Ship



Fig.2. Worldwide locations of piracy attacks for 2001

hijackings are most prevalent in the South China Sea and near Somalia.

III. MARTIME TERRORISM

The attack on the USS Cole was a horrific event of maritime terrorism. The Al Qaeda network and other terrorist groups have openly stated that they will target American transportation systems, including the sinking of ships, and will attempt to inflict maximum economic losses through their attacks. The U.S. government has reported that terrorist cells have shown interest in training to attack ships and ports and may have received scuba diving training.

In contrast to piracy, which is well characterized and occurs in certain regions of the world (see Fig. 2), maritime terrorism is not well characterized and can occur anywhere. An effective terrorist attack is one that adversely affects a country, its interests, or people. The nature of the attack may take many forms.

Potential terrorist attacks include:

- Taking hostages aboard cruise liners or ferries (e.g. hostage incident and murder aboard the Achille Lauro in the mid-80's)
- Deliberate sinkings or groundings of vessels to block harbors and/or channels

- Using ships as kinetic energy weapons to destroy other ships, bridges, port facilities, etc.
- Emptying tankers of their liquid cargo to create eco-disasters
- Conducting homicide bombings of ships (e.g. USS Cole incident) and port facilities
- Using ships to transport and perhaps detonate weapons of mass destruction and weapons of mass disruption

Terrorism experts have learned that terrorists follow a structured approach in their activities. They are patient and do their homework by collecting data, formulating an executable plan, and rehearsing the plan. Then, and only then, do they execute the plan. To defeat terrorist plots, we must think more like they do and catch them when they are vulnerable. Terrorists are vulnerable when they are collecting data and when they are rehearsing. We must recognize their activities and act swiftly and decisively.

IV. SHIP SELF DEFENSE

As stated earlier, effectively combating piracy and maritime terrorism requires cooperation among many groups at several levels. Commercial ships can and should take certain steps to protect themselves and others from attack as a part of the larger collective effort.

As with many types of security-related issues, awareness is a key component. Simply raising the level of security awareness at the deck-plate level will improve security and enhance everyone's attitudes about security. The United States Coast Guard (USCG) in its expanded role in Homeland Security is stressing the importance of "maritime domain awareness". That concept can be applied to individual ships, and indeed should apply to all of us in the maritime fields regardless of our particular functions. The concept is to make it your job to understand what is going on around you at all times and to constantly evaluate these observations. In doing so, one can adjust the nature of the security posture, select appropriate actions, and more easily spot anomalies.

A. The Ship Security Plan

There are no magic solutions that solve ship security problems. Ship characteristics vary greatly, as do their routes, cargos or services, crew composition, policies and procedures, etc. Things that might be done on one ship to improve security may not be appropriate for a different ship and crew. So, the key is to develop a ship security plan that is specific to the vessel for which it is intended. The individual ship security plan should be created to be consistent with standing policies and procedures of the owner/operator and vice versa.

A ship security plan should include as detailed a treatment as applicable of at least the following items:

- Detecting threats as early as possible
- Denying or restricting access to all or part of the ship
- Communicating to others the nature of the threat or situation being confronted
- Protecting the crew and passengers
- Protecting cargo, particularly if the cargo is hazardous
- Outlining crew actions in the event of a hostile boarding or other incident

Reference [4] suggests that a matrix be developed that groups actions as a function of threat level. The USCG's Maritime Security (MARSEC) Conditions are used to define the three threat levels:

- MARSEC Condition 1: New Normalcy (the indefinite, post September 11th threat level)
- MARSEC Condition 2: Heightened Risk (credible but undefined, non-specific threat)
- MARSEC Condition 3: Incident Imminent (credible, specific threat)

The threat levels defined above may not be appropriate for your ship, but there should be some gradation of threat level used to guide your actions. The preparations made, the types of equipment mobilized, the actions taken, etc. will vary with the nature, severity and imminence of the threat.

Another useful matrix is to categorize your security measures by whether the ship is pierside, at anchor, underway in coastal waters, or underway on the high seas. A checklist can be developed for each category that describes the equipment and procedures that are needed for that phase of the voyage.

The process of developing a meaningful ship security plan will in itself be a very beneficial endeavor. The process forces operators to think about aspects of their ship and crew, their modes of operations, their theatre of operations, etc. in ways that were previously either not thought about at all or not thought about from a security perspective.

The ship security plan should be a living document that is adapted to current conditions as frequently as necessary. For example, if a ship is tasked to serve a different port of call, the ship security plan should be revisited to see if changes are needed to address the threat environment along the new route and in the new port. Masters and crews should view the plan as a valuable tool to protect them and their ship and not as an administrative headache.

B. The Ship Security Officer

Each ship should have a designated security officer [5]. The ship security officer is responsible for the implementation and maintenance of the ship security plan, routinely inspecting the vessel, encouraging security awareness by the crew, providing training, reporting problems or deficiencies, coordinating with port facility officers, coordinating with the Master to determine best courses of action, etc.

An operator security officer should also be designated. The operator security officer is a representative from the organization in operational control over the ship while at sea and in port. He has overall responsibility for the development of ship security plans, liaison with ship security officers, and liaison with port facility officers.

C. Considerations for Ship Self Defense

Elements that should be considered when developing a comprehensive ship security plan are discussed below. The discussion points are not in any priority order. They should be used to encourage debate and discussion among appropriate persons who are preparing and eventually executing the ship security plan. Some items may not need to be addressed at all, and some may require further development to excruciating levels of detail. Of course, the list of elements can also be expanded to include items of particular importance to you that are not discussed herein.

Routing: If you can choose a route that avoids a high threat area, by all means choose that route. If your route must include a high threat area (e.g., a transit through the Malacca Straits to call on Singapore), consider your options such as maximizing the amount of daylight transit, transiting with another vessel, requesting an escort if available, etc.

Outward Appearance: Just as with common thieves who look for houses to rob that do not have deadbolts or window locks, pirates and maritime terrorists are looking for easy targets. If you demonstrate by the outward appearance of the vessel that you take security seriously, chances are good that they may look for an easier target. When in port, you can demonstrate your strong security posture by posting obvious gangway watches, having extreme amounts of exterior lighting at night, having fixed and roving patrols that are visible (and maybe some that are not), showing that your gangway watches and patrols have handheld radios and/or other forms of communications, hiring contract security guards to augment but not replace your own. Remember, you do not really know who the bad guys are.

Vigilance: Maintain a 24-hour watch on the vessel at all times. Use as many persons as needed to cover key areas and be visible. Add extra crew to the vessel if necessary for a particular voyage. Most pirate attacks occur between 0100 and 0600 local time, so heightened vigilance during these times in pirate-infested waters is particularly important [4].

Gangway Watches: Gangway watches should be posted at all times when pierside. The watch personnel should be fit, businesslike, and equipped with communications equipment. Always check ID for all persons visiting the vessel. Consider having a sign-in procedure and even consider taking instant/digital pictures of everyone visiting the ship.

Lighting: Having ample amounts of exterior lighting is a deterrent whether you are in port or underway. To discourage pirates when underway, at anchor, or pierside, use large numbers of floodlights to illuminate the decks and areas adjacent to the ship. Also, consider mounting extra searchlights and use them to illuminate approaching targets. Pirates often attack using multiple vessels so more than one searchlight is needed. If you are worried that your radar may not pick up small wooden boats, then systematically sweep the surrounding areas with the searchlights to let them know you are alert and watching.

Early Detection: Maximize your ability to detect the bad guys. This may include servicing or installing new radars, adding searchlights and floodlights, increasing crew size, etc.

Messages to the Bad Guys: Once you detect a suspected pirate or terrorist, let them know immediately that you see them. This acts as a strong deterrent. They may persist, but they also may decide to retire and wait for a less alert and determined target. Illuminate them with lights, use your radio to let them know that they have been spotted, use your loud hailer to instruct them to cease their activities immediately.

Access Prevention: Do not let the bad guys get on the ship. Once they are aboard, a new situation develops and your response options are limited. For low freeboard vessels that are a pirates dream come true, rig temporary fences at your

boarding gates and at the stern while underway. Rig and charge fire hoses at key points and man them early. Hopefully, just seeing that you plan to resist a boarding may discourage the pirates. If the pirates use grappling hooks, attempt to quickly cut the lines (this requires that the crew be equipped and required to carry large, sturdy knives). Of course, your exact course of action and the tenacity with which you fight is a matter of judgment. If it is obvious that the pirates are well armed and appear eager to use their weapons, you may choose to retire early to avoid harsh treatment, especially if it seems that you cannot be successful in repelling the boarding anyway. If the bad guys do get on the ship, prevent them from getting control of the ship. Usually this is accomplished by preventing them access to the accommodations block and the engine room through whatever means are possible on that particular ship. Emergency egress must not be hindered.

Secure Area: Establish a secure area into which the entire crew can retreat and be protected from hostile intruders. Depending on how elaborate you wish the space to be, you could equip the space with radios, GPS units, or other equipment to assist with obtaining help.

Ship Maneuvering: If pirates are approaching you, maneuver the ship erratically so that your course and speed are unpredictable and they don't know what you will do next.

Portable Equipment: To decrease your attractiveness to potential pirates, stow as much portable equipment and other items that are easy to steal in secure areas rather than keeping them in the open on deck.

Don't Advertise: Many pirates, gangs, and terrorist cells have networks of spotters that evaluate potential targets and gather intelligence on those targets, such as the vessel's itinerary, next port of call, planned route, types of cargo, number of crewmembers, etc. Do not make it easy for these operatives to get useful information.

Active Countermeasures: There are many types of countermeasures that can be use to resist attack. Firearms are a potential tool, but these are generally discouraged and are discussed elsewhere in this paper. The use of fire hoses as discussed above has been found to be effective. Using flare guns can also be effective, as can portable fire extinguishers, although the range of these extinguishers is quite limited. The use of pepper spray by the crew may also be considered. Pepper spray is very effective and is non-lethal, but is limited in range. Be sure to use the kind that shoots a stream versus a spray.

Hawse Pipes: When at anchor, utilize hawse pipe plates to seal off the opening as a possible ingress point. Alternatively, establish a running water hose at the opening to make it unpleasant to use for ingress and illuminate the area.

Anchorage: The majority of pirate attacks occur when ships are at anchor. Avoid anchorages if possible in high threat areas by steaming offshore until berthing is available.

Internal Communications: Immediately upon discovery of some sort of attack or suspicious activity, the discoverer should communicate the situation to the bridge and/or to all stations as appropriate. The use of a general alarm or code word system should be implemented to call all hands to “battle stations” when necessary.

External Communications: If your standard practices and procedures do not already include a daily (or more frequent) check-in procedure or status report, consider implementing one. Create an innocuous code word that indicates trouble on board since pirates or terrorist will likely be monitoring communications. Immediately upon the first signs of trouble, attempt to make contact with authorities to let them know of the situation you are facing. If things develop to your disadvantage, help will already be on the way. Consider having radios at locations other than the bridge, but be aware that your communications from remote locations may still be intercepted by the enemy. If time or conditions do not permit the creation and sending of a descriptive message, consider activating the emergency capabilities of the Global Maritime Distress and Safety System (GMDSS) system and/or a Digital Selective Calling VHF radio. An Emergency Position Indicating Radio Beacon (EPIRB) could even be activated. However, remember that the recipients of the message from the DSC radio or the EPIRB will not know the nature of the distress call and will probably respond by initiating search and rescue operations. A new message category is planned for implementation into the GMDSS architecture that indicates that hostile acts are involved. This added piece of information is very useful because the authorities can initiate a matched response.

Training: Just as with other aspects of maritime endeavors, training in security is essential. The master should select those portions of the security plan that demand particular attention to detail, to teamwork, etc. and require that the crew engage in periodic training in those elements. Furthermore, if you were confident enough in your abilities, conducting the training in full view of outside observers in port, you would affirm your resolve and abilities in their minds and thereby deter attack.

Firearms: The carrying and use of firearms by commercial ships is generally discouraged. However, just like the issues of domestic gun control and the arming of commercial airline pilots, the issue of mariners using guns is the subject of some spirited debates. There are valid arguments to be made on both sides of the issue. If the owner/operator decides to arm the crew, there are practical considerations that must be properly addressed. These include: selection of appropriate firearms and ammunition, training, accountability, maintenance, rules of engagement, liability, storage, life cycle cost, etc. The magnitude of the training required to be safe and effective in using firearms should not be

underestimated. This is particularly true for close quarters battle (CQB) scenarios that are likely to occur aboard a ship. In addition to initial training, on-going training is essential for effectiveness and safety to be maintained. Also, keep in mind that the use of firearms must be restricted to “within the lifelines” since only the military has the legal authority to project deadly force outside of the ship.

Interactions with Rescuers: The first responders to your emergency messages may be military or para-military forces [6]. Do not attract attention to unusual activity on or near your vessel and do not react negatively to strangely dressed persons you may see. If you hear the command to “get down” or hear gunfire, lie down with your eyes closed, your hands over your ears, and your mouth slightly open. If you hear the command to “freeze,” remain motionless or you may be shot. Do not take any photographs of the assault team or their equipment and do whatever they tell you.

D. Reporting After an Attack

If you experience an attack, the event should be reported to authorities as soon as possible. Reporting will not only assist authorities with the apprehension of criminals, but will assist governments and multi-national organizations devise policies that help curb criminal and terrorist activities.

Reports should be made to the following organizations:

- 1) The state having jurisdiction (or the nearest state if the incident occurred in international waters near a coastal state)
- 2) The IMB (603-238-5763)
- 3) The ship owner/operator’s headquarters
- 3) The USCG National Response Center (800-424-8802)
- 4) The National Maritime Intelligence Center (301-669-3261)
- 5) The US Department of Transportation Response Center Hotline (800-424-0201)
- 6) The US Maritime Administration Office of Ship Operations (202-366-5735).

A thorough report of any incident of pirate or terrorist attack should include the following information:

- Ship Name
- Flag State
- Official Number
- Ship Type
- Ship Principle Dimensions and Displacement
- Registered International Tonnage
- Ship Contact Information (call sign, phone number, etc.)
- Name and Contact Information of Ship Owner and Ship Operator (if different)
- Date and Time of Incident
- Location of Incident (Lat/Lon) and description of area

- Weather Conditions at the Time of the Incident
 - Detailed Description of the Incident including:
 - Number of pirates or terrorists
 - Type and number of craft used
 - Type and number of weapons used
 - Nationality of Attackers
 - Language Used by Attackers
 - Physical Description of Attackers
 - Detailed Sequence of Events
 - Actions Taken By Attackers and Crew
 - Outcome of the Incident (such as itemization of cargo stolen, injuries received, etc.)
 - Name of any Authorities to Which the Incident Was Also Reported
 - Actions Taken by Authorities
- [3] International Shipping Federation/ International Chamber of Shipping, Pirates and Armed Robbers: A Master's Guide, London: Marisec Publications, 1999.
- [4] American Waterways Operators, AWO Model Vessel Security Plan, Arlington, VA, April 2002.
- [5] International Maritime Organization Marine Safety Committee, Measures to Prevent Unlawful Acts Against Passengers and Crews on Board Ships, MSC/Circ.443, London, September 1986.
- [6] B.A.H. Parritt ,*Security at Sea: Terrorism, Piracy, and Drugs*, London: The Nautical Institute, 1991.

The report should be as detailed as possible. A memo is recommended rather than the use of a standard, pre-printed form. If the report is generated from scratch in a memo format, there is a greater chance that critical details will be provided. Information provided on a form is sometimes restricted to the space provided because some persons may be reluctant to attach additional sheets and take the time to provide additional information.

V. CONCLUSION

Worldwide incidents of piracy are steadily increasing. The threat of maritime terrorism is now ever present and is worldwide in scope. Many elements of the maritime community are working with a myriad of organizations to help mitigate these threats. Practical measures can be implemented aboard commercial vessels that aid the vessels in defending themselves against acts of piracy and terrorism. The measures must be vessel specific and are the outcome of developing a comprehensive ship security plan.

Acknowledgments

The authors thank Mr. Charles Dragonette of the National Maritime Intelligence Center for his time in explaining the nuances of interpreting piracy statistics and jurisdictional issues.

References

- [1] ICC International Maritime Bureau, Piracy and Armed Robbery Against Ships Annual Report, Barking Essex UK, January 2002.
- [2] Oil Companies International Marine Forum, Piracy and Armed Robbery Against Ships, London: Witherby & Co., LTD., 2000.