MARITIME SECURITY IN THE 21st CENTURY

By Lieutenant Commander David Atterbury Royal Navy (Retired)
Senior ISPS Project Manager
HudsonTrident
(Maritime Security Services)
www.hudsontrident.com

French tanker "Limburg" on fire off the coast of Yemen, following a terrorist suicide attack using a small boat.

Introduction

Ever since man first used the sea as a means of transport, the security of vessels and ports has always been a problem. But in the latter half of the 20th century vessels and ports were no longer just the preserve of pirates, stowaways and thieves, they also became the target for terrorists. However, security costs money and, although the IMO has always been concerned about security, there was little motivation in the commercial world to spend money on protecting their vessels or ports except in areas where the risk was high (e.g. The Malacca Straits). That all changed with 9/11. But the motivation to take maritime security very seriously came from governments. If airliners could be used as weapons, why not ships? Indeed a ship could be used as an even more devastating weapon. Furthermore the USS Cole and the French tanker "Limburg", showed that the terrorists had identified vessels, both in port and at sea, as 'soft' targets.

Hence, with some governments pressing for action, in December 2002 the IMO produced the International Ship and Port Security (ISPS) Code, for implementation in July 2004. Even then some ship operators and ports did not take the ISPS Code too seriously and the application of the Code became a paper, cosmetic, exercise. More and more shipping companies are beginning to realize that ISPS Code compliance is essential if they are to avoid detention and control actions being taken following a Port State Control (PSC) inspection, particularly in North American and EU countries.

Security Levels

As a brief reminder these are the 3 ISPS Code security levels. Note that the 3 Maritime Security Levels (MARSEC) in the USA are equivalent to the ISPS Code levels.

- Level 1 – Normal: The minimum appropriate protective security measures must be maintained at all times.

- Level 2 – Heightened Risk: Appropriate additional protective security measures must be maintained for a period of time as a result of heightened risk of a security incident.

- Level 3 – Incident Imminent: Further specific protective security measures must be maintained for a period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

The great majority of ships and ports operate at Security Level 1.

Port State Control

As an example of how PSC ensure the ISPS Code is implemented let us consider PSC examinations in the USA. These are conducted on behalf of the Department of Homeland Security by the United States Coast Guard (USCG).

- Targeting:
  The targeting of vessels for examination by the USCG is based on a scoring system.
  - Vessels scoring 17 points or higher are ISPS I vessels and should be examined prior to entry to port.
  - Vessels that score between 7-16 points are ISPS II vessels and are subject to examination upon port arrival.
  - Vessels scoring fewer than 7 points are ISPS III vessels and are not subject to examination unless selected for a random ISPS examination.

  There are 5 criteria that the USCG considers when allocating targeting points to a vessel:
  - Ship Management – 5 points awarded if vessel owner/operator/charterer has one denial of entry or two ISPS control actions in the previous 12 months.
  - Flag State:
    - SOLAS vessels – Between 7 points if Flag State has a Control Action Ratio (CAR = Number of major ISPS/MTSA related control actions divided by the number of ISPS/MTSA exams, times 100%) 2 times the average and 2 points up to 2 times CAR average;
    - Non-SOLAS vessels – 7 points
  - Recognized Security Organisation (RSO):
    - Automatically designated ISPS I if there are 3 or more RSO related major control actions in the past twelve months;

        - 5 Points if vessel has 2 RSO-related major control actions in the past twelve months;
        - 2 Points if vessel has 1 RSO-related major control actions in the past twelve months.
    - Security Compliance History:
        - Automatically designated ISPS I if there is an ISPS related denial of entry/expulsion from port in past 12 months;
        - Automatically designated ISPS II if matrix score does not result in ISPS I exam and no ISPS compliance exam within the past 12 months;
        - 5 points if vessel has had an ISPS/MTSA related detention in the past twelve months;
        - 2 points if vessel has had 1 or more other ISPS/MTSA control actions in the past twelve months;
        - 2 points if vessel has had at least 1 but not more than 5 ISPS compliance exams in the past 3 years beginning 1 July 2004.
    - Last Ports of Call:
        - Automatically designated ISPS I if last 5 ports are specified by Federal Register (refer to USCG HQ target list*).
        - Automatically designated ISPS II if matrix score does not result in ISPS I exam and if last 5 ports are designated ISPS II (refer to USCG HQ target list*).

* USCG Target Lists can be found on:
http://homeport.uscg.mil/mycg/portal/ep/home.do
under Maritime Security - Port State Control - Foreign Vessel Security

- Location of Examinations:
    - ISPS examinations will be conducted as follows:
        - ISPS I vessels – at sea;
        - ISPS II vessels – at pier.
    - Random, unannounced ISPS exams may occur one week after last boarding.

- PSC Guidelines for Security Examinations: The following are the areas of vessel security that PSC officers will examine.
    - ISSC and related security documents;
    - Performance of ship's security duties;
    - Access control;
    - Control of embarkation of persons / effects;
    - Control of restricted areas;
    - Control of deck areas and surrounding areas;
    - Supervision of cargo and stores loading;
    - Availability of security communication.

- Control & Enforcement: If a security problem is discovered then depending on the severity of the infringement/non-compliance, the following Control Actions may be taken.
    - Inspection of the ship;
    - Delay;
    - Detention;
    - Restriction of Operations (incl. movement of the ship);
    - Denial of Entry;
    - Expulsion.

- Examples of Deficiencies Causing Ship Detentions:

    - The gangway sign on a ship stated all visitors would receive badges to be worn while onboard. The Ship Security Plan (SSP) stated the same. But PSC officers did not receive badges to wear.
    - The vessel was not conducting security training and drills in accordance with the SSP and ISPS Code. 10 crew members, which comprise 50% of the crew, had arrived onboard and there was no documentation that they had received any security training. Furthermore the last recorded Security Drill was over 6 months previously.
    - When asked basic security questions the Master, also acting as the Ship's Security Officer (SSO), Chief Officer and gangway watch keeper gave conflicting answers with regard to number of persons on security watch and the frequency of security rounds. When asked, the Master did not know who the Recognised Security Organisation (RSO) was. The SSO had not ensured new crewmembers participated in security drills.
    - Upon embarking a vessel the PSC officers did not have his identification checked by the gangway watch keeper. The watch keeper did not check the backpack that was carried onboard. Yet according to the SSP all ID's and baggage should be checked, even at Security Level 1.
    - A vessel's crew and SSO were not familiar with the SSP and had not implemented it.

Declarations of Security (DOS)

The ISPS Code clearly sets out the requirements for DOS. But the importance of this document should not be underestimated, particularly when it is required to prove to PSC officers that a ship takes security seriously, particularly if its previous ports of call are on the USCG target list.

ISPS Compliance Measures

Therefore what can be done to meet the standards required and pass the ever more stringent checks by some Port State Control authorities and what are the implications of some of these measures upon a ship's operations.

- Ship Security Assessment (SSA): It is the responsibility of the CSO that an SSA is conducted for each ship within the company's fleet. The SSA is not only the basis upon which the Ship Security Plan (SSP) is written, but it is a document that will be checked by PSC officers. It is essential that it is comprehensive and therefore needs to be conducted by a reputable RSO.

- Ship Security Plan (SSP): This plan is the basis for all security measures and actions that a ship must implement to maintain the required standards of security. Every person onboard a ship must read it. The SSO is responsible for maintaining this document and for ensuring that it is implemented. It needs to be thorough and therefore the assistance of an experienced and reputable RSO may be required in writing it. Again, it is a document that will be inspected by PSC officers.

- Training: As was seen in the section above on examples of causes for ships to be detained, one of the areas that is examined is that of training. The training requirements are quite clearly detailed in the ISPS Code and not only will PSC

officers examine the training records but they will also assess the security knowledge of the crew. The following areas of training must be addressed:

- Company Security Officer (CSO) & Ship Security Officer (SSO): It is not only mandatory under the ISPS Code that the CSO and SSO receive training but the training courses must be approved by the Flag State. The ISPS Code clearly indicates the knowledge requirements and the IMO has given guidance on what is to be included. One topic in these courses is "Train the Trainer", so that the CSO and/or SSO are capable of conducting the mandatory security training for ship crews.

- Security Awareness Training: Security is everyone's business. And the ISPS Code requires that all crew members receive security awareness training which is properly recorded and documented.

  It is also important that between the CSO and SSO they conduct regular security threat assessments on sea areas and ports and brief the crew accordingly.

- Security Drills and Exercises: Not only is it necessary to give the crew training, but it is also an ISPS Code requirement that regular Drills and Exercises are conducted. CSO and SSO must be trained on how to conduct these.

Besides Training, there are 6 other areas that require serious attention when ship security is considered:

- Access Control: This is an area that can provide problems when, with a limited crew, ships are required to maintain a gangway watch in port and conduct ID and baggage checks. This requirement must be discussed between the CSO, SSO and the PFSO of a port to see if a port can assist. In the end, hiring security guards may be the only option, particularly whilst a ship is fully engaged in cargo operations. But this can be expensive.

  Furthermore, it is not just the gangway that needs to be controlled but measures need to be taken to prevent access to the ship and areas within the ship. It is also not just a problem that needs to be considered whilst in port, but access control should be considered whilst at sea too. This is particularly so in sea areas where there is a high security risk.

- Monitoring Security: An area of security that is closely linked to Access Control, it is also one that can be manpower intensive. However, electronic aids such as CCTV and Intruder Detection systems can relieve some of the burden. The IMO is even advising that in areas where piracy is prevalent ships consider installing yacht radars to cover the main radar blind arcs.

- Restricted Areas: The reasons for identifying areas within a ship where access is restricted are stated below. Such areas must be listed in the SSP.
  - Preventing unauthorized access;
  - Protecting crews, passengers and port personnel;
  - Protecting sensitive security areas within a ship (e.g. the Bridge, Radio Room, Engine Room, etc.);

- Protecting ship's cargo and stores from tampering.

- Cargo Handling: This is an area of great opportunity to the terrorist and another area that requires particular security awareness from a ship's crew. The security measures for cargo handling in the SSP should be designed to:
  - Prevent tampering;
  - Prevent cargo that is not meant for carriage from being accepted and stored onboard.

- Ship's Stores & Bunkers: As with cargo handling, this is another area that requires particular security awareness from a ship's crew. Too often ships take the delivery of stores for granted and also rely on the port's security organisation to have done the checking. A ship should have measures and procedures for:
  - Checking ship's stores and package integrity;
  - Prevent ship's stores from being accepted without inspection;
  - Prevent tampering;
  - Prevent ship's stores from being accepted unless ordered.

- Unaccompanied Baggage: The SSP must specify procedures for ensuring that baggage which arrives unaccompanied (e.g. personnel effects of a crew member or passenger) is identified and searched before it is accepted onboard. It need not be checked by both the port authority and the ship but ships must liaise with a port's security organisation regarding unaccompanied baggage. Quite often a port may have screening equipment (e.g. X-ray scanners) that are not available to ships.

Conclusion

Maritime security is not rocket science. Its successful implementation depends on knowledge of basic procedures, common sense and an awareness of the threat. But personnel should have the attitude that security is someone else's responsibility and they should not assume that others have done their job. Increasingly ship security inspections by PSC are becoming more stringent and detentions more frequent. Therefore it has significant commercial implications.

The ISPS Code was born out of terrorist activity and is designed to counter the terrorist threat. However, if a ship can protect itself against terrorism, then it is also protecting itself against piracy, theft and stowaways.