Other Maritime Security Threats

1. Introduction

This section deals with maritime security threats other than piracy and armed robbery, and, the fundamental requirements and recommendations to ensure that companies and ships can respond in a proportionate and dynamic way. Whilst this guidance has been developed for the specific purposes of mitigation against attack by pirates and armed robbers, experience has shown that some of the procedures and measures described can be applied to mitigate against other maritime security threats, depending on the threat profile.

The purpose of this section is to assist companies and Masters in identifying and preparing for maritime security threats other than piracy and armed robbery that may be encountered during a voyage. It also identifies the resources by which they can assess the risk to the ship and crew and identify measures to avoid and mitigate against the threat in the event that it materialises.

2. Differences between Piracy and Armed Robbery and, non-Pirate Threats

Other maritime security threats differ from piracy and armed robbery in a number of ways, and this affects the measures that can be taken to mitigate against them. In the case of pirates and armed robbers, the intent and methodologies of the attackers are well established across a number of geographical locations, as are the mitigation measures for deterrence and avoidance. By contrast, other threats are unpredictable, can emerge suddenly and may disappear just as quickly. The methodologies employed by the perpetrators behind these threats are also likely to vary significantly, and as such appropriate mitigation measures will vary depending on the nature of the threat.

3. Types of Maritime Security Threats other than Piracy and Armed Robbery

The nature of a threat to the security of the ship will vary depending on circumstance, as described above, however, in broad terms, threats can be grouped according to the three definitions provided below. It should be noted that this list is not extensive and that other threats may emerge or be identified through risk assessment.

3.1 Terrorism

There is no commonly agreed definition of terrorism, however, in the context of maritime security it would generally mean attacking the ship, its crew or passengers in order to serve a political or ideological aim. Historically, there have been a number of terrorist incidents against shipping which have demonstrated the variety of methodologies at the disposal of terrorist organisations. By comparison with land-based incidents, shipping has a markedly low incidence of attack by terrorists, but the threat remains, and companies and ships' crews should remain vigilant and actively apply the provisions of the ISPS Code (see below). Relevant guidance may be issued by States, regional organisations and Industry bodies e.g. the Industry Releasable Threat Assessments and Bulletins.

3.2 War and warlike activity

Areas of conflict , either international conflict or civil war, can present risks to ships and their crews. The extent of this risk will depend on the nature of the conflict and the modus operandi of the forces involved. Areas of enhanced risk to shipping due to perils insured under war risks are detailed in the Joint War Committee's Listed Areas and companies should refer to this as part of the risk assessment. Information is also likely to be provided by flag States under the requirements of the ISPS Code.

3.4 Cyber attacks

Ships are increasingly using systems that rely on digitisation, integration, and automation, which calls for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet. This brings the greater risk of unauthorised access or malicious attacks to ships' systems and networks. Risks may also occur from personnel accessing systems on board, for example by introducing malware via removable media. The safety, environmental and commercial consequences of not being prepared for a cyber incident may be significant. The shipping industry *Guidelines on Cyber Security Onboard Ships* should be rigorously followed to ensure companies and ships are prepared for the risk of cyber attack.

4. ISPS Code

The International Ship and Port Facility Security (ISPS) Code and associated 2002 SOLAS Amendments were developed in response to the terrorist attacks of 11 September 2001 and the perceived risks to ships and the danger of ships being used for terrorist purposes. The Code and amendments set out the statutory requirements for shipping companies, ships and their crews with respect to maritime security.

The Regulations and Code enforce requirements on flag States, port States, shipping companies, ships and port facilities in order to ensure the security of the ship-port interface. Some flag Administrations may also designate security levels for specific sea areas. Under the Code all ships must have a flag-approved Ship Security Plan (SSP) which determines the measures to be applied at any one of three maritime security (MARSEC) levels. The flag State will advise the ship of the MARSEC level during its passage and it is the ship's duty to comply by enacting the relevant measures as set

out in their SSP. The process is overseen by the company and Ship Security Officers and the ship's Master.

Full application of the provisions of the ISPS Code and, in particular, the thorough development and robust application of the SSP is fundamental to ensuring ship security. Whilst compliance with the Code is mandatory, there is nothing to prevent a company, CSO or Master enacting further measures beyond those determined by the MARSEC Level to ensure the safety and security of their ship, as set out below.

5. Identifying and Preparing for Other Maritime Security Threats

The following sections explain the measures that should be applied by the company, CSO and Master to ensure that a ship is aware of and appropriately prepared for any threats that may be encountered during its voyage to the fullest extent possible. The processes which should be used correspond to those described in sections 3–9 of this guidance.

5.1 Threat and Risk Assessment

The threat and risk assessments, as covered under section 4 of this guidance should identify and account for the risk to the ship from other maritime security threats. In determining this risk, the company, CSO and Master should follow the relevant guidance and latest updates from their flag States, insurance, national and regional authorities, military forces, and private security information providers.

5.2 Company and Master's Planning

It is important that as part of risk assessment and planning, the company, CSO, SSO and Master consider the threats that may be encountered during the voyage. This will provide a clear indication of mitigation measures to be applied.

5.3 Ship Protection Measures

The threat assessment and company planning should indicate the likely presence of other maritime security threats during a voyage, and will determine the ship protection measures to be applied. It should be recognised that whilst some SPMs for piracy and armed robbery, such as increased watches and denial of access are likely to be useful in mitigating against some threat types, some measures are unlikely to be effective when the ship is faced with threats of a markedly different methodology or intent.

5.4 Brief crew, check equipment and conduct drills

Crews should be briefed on the preparations and drills to be conducted to mitigate against identified threats other than piracy and armed robbery, prior to arrival in an area of risk.

5.6 Privately Contracted Armed Security Personnel

It is important that companies, CSOs and masters are fully aware of caveats placed on the use of armed security teams under flag State licenses.

5.7 Action when faced with an incident

As described above, the actions to be taken when an incident is under way will be determined by the SSP.

5.8 Post Incident Reporting

Any security incidents should be reported to the flag State and the relevant local authority. Where a VRA or other reporting area exists, then a report should also be provided to the relevant regional organisation as appropriate.