Global Counter Piracy Guidance for Companies, Masters and Seafarers

Produced and supported by:

BIMCO · CDI · CLIA · International Chamber of Shipping · INTERCARGO · IFSMA · IGP&I International Group of P&I Clubs · IMCA · InterManager · ICC International Maritime Bureau · IPTA International Parcel Tankers Association · IMEC · ISWAN · INTERTANKO · Joint Hull Committee · Joint War Committee · OCIMF · SIGTTO · WORLD SHIPPING COUNCIL PARTNERS IN TRADE · MARITIME SECURITY CENTRE · INTERPOL · ROYAL NAVY

Global Counter Piracy Guidance for Companies, Masters and Seafarers

First Published June 2018

Authors: BIMCO, ICS, IFSMA, IGP&I, INTERTANKO, INTERCARGO, INTERMANAGER and OCIMF

The authors also acknowledge the use of the Regional Guide to Counter Piracy and Armed Robbery against Ships in Asia.

Published by

Witherby Publishing Group Ltd
4 Dunlop Square,
Livingston EH54 8SB,
Scotland, UK

+44 (0)1506 463 227
info@witherbys.com
witherbys.com

Printed and bound in Great Britain by Bell & Bain Ltd, Glasgow

Contents

Fundamentals

The fundamental requirements of best practices to avoid attack by pirates and armed robbers are:

1. Conduct thorough, ship-specific pre-voyage threat and risk assessments to identify appropriate Ship Protection Measures (SPMs).
2. Implement SPMs as identified in the pre-voyage risk assessment. Companies may always wish to consider new and innovative SPMs beyond the scope of this guidance and provide additional equipment or manpower as a means of further reducing risk. If attackers cannot board a ship they cannot hijack it.
3. Ships should register in accordance with the requirements of any Voluntary Reporting Area (VRA) they are transiting.
4. Ships are strongly encouraged to report daily when operating in in a VRA either by email or phone using the relevant Ship Position Reporting – Daily Position. Particularly vulnerable ships will be noted and monitored.
5. A proper, visible lookout is the most effective method of ship protection. It can help identify a suspicious approach or attack early on, allows defences to be deployed and, can serve as an effective deterrent to would-be attackers.

IF ATTACKERS CANNOT BOARD A SHIP THEY CANNOT HIJACK IT

Aide Memoire

AVOID BEING A VICTIM OF PIRACY AND ARMED ROBBERY	
Do Not Be ALONE	• Report to the relevant reporting centre and Register Transit • Co-operate with military or other counter piracy services where such missions exist • It is recommended to keep AIS turned on
Do Not Be DETECTED	• Keep track of NAVWARNS and visit relevant websites for known pirate operating locations • Consider the appropriate level of lighting to be used in areas of risk
Do Not Be SURPRISED	• Increased Vigilance – lookouts, CCTV and Radar
Do Not Be VULNERABLE	• Use visible (deterrent) and physical (preventative) Ship Protection Measures • These could include: razor wire, use of water/ foam etc. • Provide additional personal protection to bridge teams
Do Not Be BOARDED	• Increase to Maximum speed • Manoeuvre the ship without severely reducing speed
Do Not Be CONTROLLED	• Follow well practiced procedures and drills • Use of Citadels (Only with prior agreement Master/Company and fully prepared and drilled – noting a Naval/Military response is not guaranteed) • Deny use of tools, equipment and access routes

Section 1

Introduction

Piracy and Armed Robbery at Sea

Piracy and armed robbery at sea is an organised and persistent criminal activity prevalent in many parts of the world. Attackers are often aggressive and subject their victims to violence and ill treatment. Ships have been hijacked, either for a ransom payment for the release of captive seafarers, theft of cargo or both. Some seafarers have been held hostage for several years.

Experience shows that applying the recommendations in this guidance will assist ships to detect, avoid, deter or delay attacks.

Not all mitigation measures in this guidance will be applicable to every ship type or in every region. Companies, CSOs and Masters should use this guidance when conducting threat and risk assessments.

The purpose of this guidance is to protect seafarers, the ship and cargo and, to facilitate threat and risk assessment and planning for voyages transiting areas where the threat of attack by pirates and armed robbers exists.

This guidance consists of:

- General advice and recommendations that are common to mitigate against attack by pirates and armed robbers;
- Guidance on threat and risk assessment, planning and the implementation of self-protection measures;
- Appendix A providing information on other security threats and the fundamental requirements and recommendations to ensure that companies and ships can respond to those threats in a proportionate and dynamic way; and

- Annexes providing information on regions where there is a risk of piracy and armed robbery and where prior planning and preparation before transiting the region is recommended.

This guidance is complementary to other industry regional guidance and that issued by international regional organisations such as the Regional Guide to Counter Piracy and Armed Robbery against Ships in Asia produced by ReCAAP ISC in collaboration with other regional organisations.

This guidance also complements guidance on piracy and armed robbery provided in the latest IMO MSC Circulars (see the IMO website at www.imo.org) and should be seen as complementary to IMO MSC.1/Circ.1334 as amended.

Other sources of information include:

Maritime Security Centre – Horn of Africa website (www.mschoa.org)

UKMTO (www.ukmto.org)

NATO Shipping Centre (www.shipping.nato.int)

IMB Piracy Reporting Centre web site (https://www.icc-ccs.org/index.php/piracy-reporting-centre)

Information Fusion Centre Singapore (www.infofusioncentre.gov.sg)

ReCAAP website (www.recaap.org).

Nothing in this guidance detracts from the Master's overriding authority and responsibility to protect the crew, ship, and cargo.

A review of the guidance will be carried out by the authors after one year and thereafter bi-annually. Unless there is an immediate and urgent issue requiring change.

Other Maritime Security Threats

Whilst this guidance has been developed for the specific purposes of mitigation against attack by pirates and armed robbers, experience has shown that the some of the procedures and measures described can be applied to mitigate against other maritime security threats, depending on the threat profile.

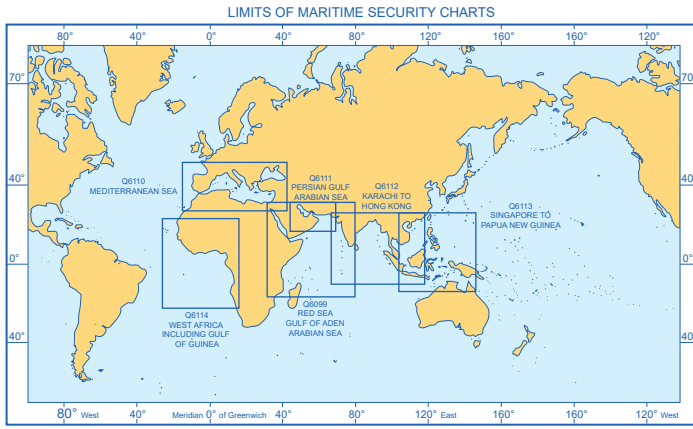
Appendix A provides guidance on other security threats to assist companies, CSOs and Masters in identifying and preparing for other maritime security threats that may be encountered during a voyage, and identifying the resources by which they can assess the risk to the ship and crew and identify measures to avoid and mitigate against the threat in the event that it materialises.

Piracy and Armed Robbery against Ships Worldwide

Pirates and armed robbers are known to conduct attacks from small fast craft and skiffs, sometimes launched from motherships, which are easier to operate in relatively calm sea conditions. It should be noted that in general, the calmer the sea state, the greater the risk of attack.

Piracy and armed robbery most often occurs in the areas described on the following admiralty maritime security charts:

- The Western Indian Ocean (WIO) – Q6099 (see Annex A)
- The Gulf of Guinea (GoG) – Q6114 (see Annex B)
- SE Asia (SEA) – Q6112, Q6113 (see Annex C)



Q6099	20°S - 31°N, 31°E - 80°E	Q6111	15°N - 31°N, 47° 40E - 70°E	Q6113	16° 53S - 26°N, 130°E - 146° 39E
Q6110	27°N - 47° 30N, 15°W - 42°E	Q6112	15° 07S - 25°N, 65°E - 118°E	Q6114	25°S - 23°N, 25° 30W - 18° 30E

The areas covered by the charts should not be regarded as exhaustive – piracy and armed robbery is a dynamic International crime which may affect other areas. In the event of piracy and armed robbery emerging as a persistent threat in other regions, this guidance will be updated accordingly. The industry website www.maritimeglobalsecurity.org should be viewed for the latest regional guidance.

These charts provide guidance including details of information sharing and voluntary reporting and, should be used in conjunction with this guidance. Notices to Mariners will advise of changes.

The charts also provide details of Maritime Security Voluntary Reporting Areas (VRAs) and reporting and registration requirements which ships should adhere to. This ensures that military forces in the region are aware of the ship's passage plan, and its vulnerability to attack.

The latest information on locations within a VRA where pirates are likely to operate can be obtained from the sources listed in the annexes prior to completing the threat and risk assessments (see section 4). It is also important ships are prepared to respond at short notice to avoid attack when information is provided by navigational warnings (Navtex), Inmarsat Safety Net Broadcasts and/or Naval/ Military forces.

Information is also available through International Maritime Bureau Piracy Reporting Centre (IMB PRC), which is an independent, not for profit and non-governmental agency providing a 24-hour manned service to shipmasters and ship owners to report any incident of piracy and armed robbery occurring anywhere in the world.

Joint War Committee Listed Area

The insurance community lists an area of perceived enhanced risk in the region. Ships entering the area would need to notify their insurers and additional insurance premiums may apply. The Joint War Committee (JWC) comprises underwriting representatives from both Lloyd's and the International Underwriting Association representing the interests of those who write marine hull war business in the London market. The geographic limits of all JWC listed areas can be found on their website: www.lmalloyds.com/lma/jointwar.

Voluntary Reporting

A major lesson learnt from operations against piracy and armed robbery to date is the importance of liaison with the military and law enforcement. This is an essential part of self-protection that applies to all ships. To ensure these forces are aware of the intended sea passage and to understand the ships' vulnerability to an attack, ships are encouraged to report to the centres overseeing the Voluntary Reporting Areas (VRAs). This information is essential to enable the centres to best use any assets available to them and to assist in an emergency. Once ships have entered a VRA it is important that they continue to report while transiting within the area. This will allow the reporting centres to update the ship of any maritime security related incidents or threats in that region. The four key centres are as below:

- For the Western Indian Ocean, the MSCHOA and UKMTO voluntary registration and reporting scheme in the WIO (chart Q6099). It is extremely important CSOs and Masters understand the differences outlined in this chart and those below. A specific and detailed High Risk Area (HRA) is outlined and there are important reporting procedures to be followed in order to monitor and give guidance at short notice on threats in the HRA. Ship reporting is the major indicator to MSCHOA on the level of implementation of BMPs and the only area where it is monitored to this extent. See Annex A for further detail.
- For the Gulf of Guinea, the MDAT-GOG voluntary registration and reporting scheme (Admiralty chart Q6114 and French Navy Hydrographic SHOM Chart 8801CS). It is strongly encouraged that the reporting requests for information are implemented by all ships transiting the VRA. See Annex B for further detail.

- For South East Asia, the Singapore Information Fusion Centre (IFC) voluntary community reporting scheme (charts Q6112 and Q6113). This VRA is extremely large and should be considered in conjunction with the listed 'areas of concern'. The differences between the transit reporting guidance to the IFC and requirements for immediate incident reporting and procedures as highlighted by ReCAAP ISC, should be noted carefully by Masters and CSOs. See Annex C for further detail.

The Admiralty Charts referenced above provide the mariner with maritime security reporting information to compliment effective voyage planning through the regions. Due to the risk of piracy and armed robbery, and the complexity of security threats in the regions, the Admiralty Charts should be used in conjunction with Admiralty Notices to Mariners, Safetynet Service warnings and Navtex messages. The VRAs as shown on the charts clearly define an area, so that companies and ships transiting, trading or operating in these regions can join a trusted reporting scheme.

Positional data, suspicious activity and incidents reported by shipping in the VRAs, using the forms on the Charts, assist in the creation of a detailed and accurate regional maritime security picture. The analysis is used to produce security recommendations that are shared with seafarers, companies and law enforcement agencies to improve threat awareness and, incident response.

Ships are strongly encouraged to register and report with the respective reporting centres as appropriate and, then send regular reports.

Section 4

Company Threat and Risk Assessment

This section details the procedures that should be undertaken by the CSO and Master in cooperation to identify the appropriate Ship Protection Measures to be applied to a voyage through an area or areas of risk from piracy and armed robbery.

Threat Assessment

The threat assessment should include threats of piracy and armed robbery so that its output will inform the risk assessment.

A threat is formed of intent, opportunity and capability. Intent and capability cannot be mitigated by masters or CSOs. Therefore, mitigation against the opportunity for an attack is the focus of this guidance, risk assessments and any subsequent SPMs.

In the context of piracy and armed robbery, capability means that attackers have the physical means to conduct an attack, intent is demonstrated by continued attacks, opportunity is what is mitigated by the company, ship and crew through application of the measures described in this guidance.

In addition to the information provided in this guidance, supplementary information about the characteristics of the threat, specific or new tactics, and regional background factors may be sought from Regional Reporting Centres and Organisations as listed in the sources detailed at the annexes, Shipping Association

websites, commercial intelligence providers or local sources e.g. ships' agents.

Risk Assessment

Risk assessment is an integral part of voyage planning within a safety management system. All voyages require thorough advanced planning and risk assessment using all available information. The risk being evaluated should include likelihood of harm to the crew or ship from attack by pirates and armed robbers. The risk assessment must reflect the prevailing characteristics of the specific voyage, ship and operations and not just be a repetition of advice e.g. relating to different geographical regions and different pirate modus operandi. Detailed guidance on preparing risk assessments can be found from a variety of sources including the ISPS code.

4.1 Risk assessment considerations for the Company

Like the Ship Security Assessment described in the ISPS Code, the risk assessment for the risk of piracy and armed robbery should include, but may not be limited to, the following:

- The threat and potential areas of increased risk (who are the pirates or armed robbers, what do they want to achieve, how do they attack, how do they board, which weapons do they use etc.) Companies should use the sources listed at the annexes to do this.
- Background factors shaping the situation (likely visibility, sea-state, traffic patterns e.g. other commercial ships, local patterns of life including fishermen and, other local maritime crime).
- Co-operation with military or other security services where such missions exist.

- The ship's characteristics/vulnerabilities/inherent capabilities to withstand the threat (freeboard, speed, general arrangement etc.).
- The ship's and Company's procedures (drills, watch rosters, chain of command, decision making processes etc.).

The risk assessment should take into consideration any statutory requirements, in particular those of the flag and/or the coastal State.

A key output of any risk assessment process should identify whether additional mitigation measures are required to prevent attack.

Section 5

Company Planning

5.1 Company planning prior to entering an area of increased risk

This section details the procedures that should be undertaken by the company prior to a ship entering an area of increased risk identified through the risk assessment in order to mitigate against the risk of attack. It should be noted that pirate and armed robbery risk will vary across regions.

5.1.1 Register ship with relevant reporting centre

It is strongly recommended that companies register for access to all websites offering additional and updated information prior to entering an area of increased risk identified through the risk assessment. For example, the restricted section of the MSCHOA website and, the UKMTO website contain additional and updated information. Note that this is not the same as registering a ship's movement – see below.

5.1.2 Obtain latest threat and risk information from designated regional sources

Great care should be taken in voyage planning and the company should obtain the latest threat information from the relevant websites (see the annexes as appropriate).

5.1.3 Review Ship Security Assessment (SSA) and Ship Security Plan (SSP)

After completing the risk assessment, the company should review the ship security assessment and implementation of the ship security plan, ensuring that any necessary follow-up actions are taken as appropriate.

5.1.4 Put ship protection measures in place

The company should ensure the SSP highlights where and when SPMs and vessel hardening are to be in place for passage through

an area of increased risk and, that this is exercised, briefed and discussed with the Master and the Ship Security Officer (SSO).

5.1.5 Monitor piracy related websites for current threats

Ensure that crews are briefed of any threats of piracy and armed robbery which may be encountered during the voyage. Company procedures should stipulate masters to monitor all NAV WARNINGS – SAT C (NAVTEXT in limited areas) as appropriate. (see the annexes as appropriate).

5.1.6 Offer guidance to the Master as to recommended route

Offer the Master guidance regarding recommended routeing through areas of increased risk identified through the risk assessment. Guidance should be provided on using recommended transit corridors or other supported routes (e.g. a Group Transit or National Convoys where these exist). If anchoring, consideration should be given to the use of protected anchorages where available recognising that standards of protection vary widely. The company should appreciate that the voyage routeing may need to be reviewed and amended at short notice in light of updated information.

5.1.7 Plan to maintain security of critical information

To avoid critical information falling into the wrong hands, consideration should be given to ensuring that:

- Communications with external parties are kept to a minimum with close attention paid to organising rendezvous points and waiting positions; and
- Email correspondence to agents, charterers and chandlers should be controlled and information within the email kept concise, containing the minimum information that is contractually required.

5.2 Company planning on entering an area of increased risk

Ensure that the appropriate registration and/or reporting forms have been submitted in accordance with the applicable reporting recommendations.

Section 6

Ship Master's Planning

6.1 Ship Master's planning prior to entering areas of increased risk

This section details the procedures that should be undertaken by the ship's Master prior to a ship entering an area of increased risk identified through the risk assessment, in order to mitigate against the risk of attack.

6.1.1 Implement SPMs

SPMs should be implemented as determined through the risk assessment.

6.1.2 Brief crew, check equipment and conduct drills

Crew should be briefed on the necessary security arrangements identified in the SSP. Drills should be conducted prior to arrival in an area of increased risk as identified through the risk assessment. Drills should be unannounced, to ensure crew respond appropriately in the event of an actual attack. If necessary, drills should be repeated in order to improve response times. Personnel should be briefed on their duties, including ensuring familiarity with the alarm signal indicating an attack, an all-clear signal and the appropriate response to each. Consideration should also be given to the following:

1. Testing the SPMs and physical security including all access points.
2. Removing unnecessary equipment from the upper deck.
3. Securing the accommodation block.
4. Testing Ship Security Alert System (SSAS) (giving prior warning).
5. Testing all communications equipment, alarms, etc.
6. Testing all deck lights and search lights.

Ensure that crew members will not be trapped inside a ship, during an attack or during an emergency for example fire or flooding.

The location of any Safe Muster Point and/or Citadel should be known to all crew members. This location should only be shared with relevant third parties such as military or law enforcement authorities responding to an incident. The location should not be shared freely with any third party e.g. port authorities, stevedores, etc.

6.1.3 Emergency Communication Plan

Masters are advised to ensure that an Emergency Communication Plan has been developed in accordance with the risk assessment, that includes all essential emergency contact numbers and prepared messages, and which should be ready or permanently displayed near all external communications stations (e.g. telephone numbers of regional centres, CSO, IMB PRC etc.).

6.1.4 Automatic Identification System

It is recommended, subject to frequent assessment, that Automatic Identification System (AIS) transmission is left on throughout any and all areas of risk, but that it is configured to transmit ship's identity, position, course, speed, navigational status and safety-related information only. It should be recognised that certain flag and/or coastal State regulations can require AIS to be left on.

6.1.5 Define the ship's Ship-to-ship Transfer (STS)/Single Buoy Mooring (SBM) policy

The following should be considered when planning Ship-to-ship Transfer (STS)/Single Buoy Mooring (SBM):

1. During an STS operation it is essential that the lookout is coordinated between the tankers and any standby ships. This is particularly important as there may be restrictions on operating radar during an STS operation.

Consideration should be given to the issuing of hand held night vision optics to assist with the identification and early warning of unidentified small craft.

2. When conducting STS operations it is recommended that the Master establishes communications with the shore authority regardless of where the STS is taking place, but that contractor/agent communication should be as late as possible in the proceedings. All communications should be kept to a minimum to prevent unauthorised receipt of information.
3. Consider the use of protected anchorages where available recognising that standards of protection vary widely.
4. Consideration should be given to radar watches, Lighting arrangements and the notice for getting underway.

Use of codewords may be considered appropriate if it is believed that communications are likely to be compromised.

6.2 Ship Master's planning on entering an area of increased risk

This section details the procedures that should be undertaken by the Master on the ship's entry into an area of increased risk as identified through the risk assessment and during transit in order to mitigate against the risk of attack. When transiting areas of increased risk identified through the risk assessment, further briefing and checks are likely to be required prior to entering them.

6.2.1 Submit initial Ship Position Report Form

If the voyage includes the transit of a VRA the Master should submit a "Ship Movement Registration" form to the relevant reporting centre (see the annexes as appropriate).

6.2.2 Implement the measures required by the risk assessment

The Master should ensure that the measures identified in the risk assessment have been effectively implemented.

6.2.3 Implement the Communications Policy

Master and Crew should ensure critical information does not fall into the wrong hands e.g. to protect the release of sailing times and routeing information (see section 5.1.7).

Consideration should be given to minimising the use of VHF. Use email or a secure satellite telephone instead. Where possible only answer known or legitimate callers on the VHF radio, bearing in mind that imposters are possible.

6.2.4 Maintenance and engineering work should be undertaken within any restrictions imposed by the voyage risk assessment

When operating in areas of increased risk identified through the risk assessment – the following should be considered:

1. Any work outside of the accommodation is strictly controlled and similarly access points limited and controlled;
2. All Engine Room essential equipment to be immediately available;
3. No maintenance on essential equipment.

6.2.5 Carefully review all warnings and information

The Master (and company) should appreciate that the voyage routeing may need to be reviewed in light of updated information received. This information and warnings may be provided by a number of different means, including navigational warnings – Sat C (and NAVTEXT in limited areas) as well as direct messaging in certain areas. It is important all warnings and information are carefully reviewed.

6.2.6 Consider speed and manoeuvring

Increasing speed makes it difficult for an attacker to board. Engines should be ready for immediate manoeuvre. The passage speed of the ship will be determined by the risk assessment. Consider planning on increasing ship speed, particularly if there is a low freeboard. Ships should spend as little time as possible stationary, drifting or operating at low speeds – especially when working inshore. If stationary, the use of protected anchorages should be considered, where available, recognising that standards of protection vary widely.

- The ability to get underway and/or increase to a maximum safe speed as quickly as possible when operating in areas of increased risk identified through the risk assessment is required is of the utmost importance. This will open the distance from any possible attack and make the ship more difficult to board.
- Manoeuvring away from a threat if detected at range increases the time taken for the attacking vessel to close its distance from the ship. Similarly making best use of sea conditions to create the most difficult transit conditions for small craft is another option. Aggressive manoeuvring when a small boat is close to or alongside makes the use of ladders and climbing ropes more difficult for the pirates.

Freeboard

- A ship underway is most easily boarded at the lowest point of its freeboard. Additional SPMs should be used to deny pirates access at these points.
- A ship's freeboard height may change during a voyage. When changes in freeboard occur the effectiveness of SPMs will need to be considered during the risk assessment.

Location and Time at Anchor

- Keep time at anchor to a minimum where possible.
- Consider appropriate use of lighting (see section 7.10).
- Consider use of “safe anchorages” where they are provided. Information on safe anchorages is provided in local Notice to Mariners or Admiralty Charts (see annexes).
- The location of the anchorage, STS operation and SBM are also important factors in mitigating risks against attacks on the ship. Ships are most vulnerable when stopped in the water, drifting, at anchor, carrying out Ship to Ship (STS) transfer, ship’s ballast management operations or, slowing down for pilot transfer.

Coordinated Arrival

- Passage plans should be designed to result in arrival at a pilot station ‘just in time’ to avoid drifting or waiting in a vulnerable area. Many ships wait offshore and transit to meet the pilot at high speed. A period of high vulnerability is when the ship slows down to embark the pilot. Tendering early notice of readiness can be beneficial to prevent unnecessary loitering or drifting.
- Do not drift. Avoid being underway without making way.

Sea State

Attackers are known to conduct attacks from small fast craft, sometimes from motherships, which are easier to operate in more benign conditions. The calmer the sea state, the greater the risk of attack.

6.2.7 Increase vigilance during STS/SBM operations

The STS/SBM policy should be fully implemented (see section 6.1.5).

6.2.8 Submit daily position report to relevant reporting centre

When operating inside a VRA, ships are strongly encouraged to report daily relevant reporting centre by email/fax.

6.2.9 Consider utilisation of Convoy systems where available

In certain areas of risk military forces may offer assistance in the form of group transits and national convoys.

Section 7

Ship Protection Measures (SPM)

7.1 Introduction

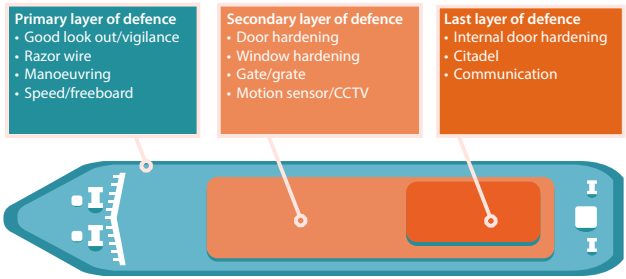
This section focuses on measures that can be taken by the ship's crew to mitigate against attack.

The guidance is based on global experience of attacks by to date. Not all methods will be applicable to all regions or ship types, and the measures applied on any one ship will be dependent upon the outcome of the risk assessment.

When considering ship protection measures (SPM) it is important to recognise that ships can be attacked both when underway and stationary (at anchor, carrying out STS or SBM operations or drifting).

Many companies have their own detailed guidance on ship hardening procedures – all based on their risk assessment. The risk assessment recommendations and guidance should be based upon the concept of 'Defence in Depth', and a 'Layered Defence.' The premise of this concept is that any robust security system must be resilient to partial failures and that multiple layers of defence make the system less predictable for any would-be attackers, therefore making the system more difficult to circumvent.

Companies may wish to consider making further alterations to the ship beyond the scope of this guidance, and/or provide additional equipment and/or manpower as a means of further reducing the risk of attack. If pirates and armed robbers are unable to board a ship they cannot hijack it. The effective implementation of these SPMs has proven successful in deterring and/or delaying attack.



An example of "layered" defence

7.2 Watch keeping and enhanced vigilance

Before entering any areas of increased risk identified through the risk assessment, one of the outcomes of the risk assessment is which SPMs are appropriate for the risk of attack. Preparations should be made to support increased vigilance by:

- Providing additional lookouts for each Watch. When stationary crew should be monitoring the water around the ship – it is essential that an all-round lookout is maintained from an elevated position. The lookout team should keep in regular contact with the Officer of the Watch.
- Considering a shorter rotation of the Watch period in order to maximize alertness of the lookouts.
- Ensuring that lookouts are briefed by the Officer of the Watch at the start of each watch on the tactics of local pirates and armed robbers.
- Maintaining sufficient binoculars for the Bridge Team, preferably anti-glare. The use of hand held thermal imagery optics, night vision aids/equipment could also be considered as they provide a reliable all-weather, day and night surveillance capability.

- Maintaining a careful Radar Watch, monitoring all Navigational Warnings and monitoring communications, particularly VHF and GMDSS alerts.
- Well-constructed dummies placed at strategic locations around the ship can give the impression of greater numbers of crew on watch. This is very effective when stationary.

- When in port or at anchor regular security rounds should be conducted. The accommodation ladder should be kept at main deck level and lowered when required only. A gangway watch should be maintained at all times when the accommodation ladder is lowered.
- Approaching vessels should be challenged to prove their identity before they are allowed alongside.
- Consider enhancing already fixed technology such as CCTV for better monitoring and fixed lighting such as the ship search light. The latter has proven effective in deterring approaches from the stern.

- It should be noted that lower sea states can also improve detection range of criminal craft both by radar and visually.

A proper, visual lookout is the most effective method of ship protection. It can help identify a suspicious approach or attack early on, allows defences to be deployed and, can serve as an effective deterrent to would-be attackers.

7.3 Enhanced bridge protection

The bridge is usually the focal point of an attack. In some situations, pirates direct their weapon fire at the bridge in an attempt to try and stop the ship. If the ship is at anchor the bridge may not initially be the focus during a boarding attempt. However, if attackers are able to board the ship, they usually make for the bridge. The following protection enhancements might be considered – particularly in those areas where weapons are often used in the attack (see the annexes as appropriate):

- Bridge windows are laminated but further protection against flying glass can be provided by the application of blast resistant film.
- Fabricated metal (steel/aluminium) plates for the side and rear bridge windows and the bridge wing door windows, which can be quickly secured in place in the event of an attack can greatly reduce the risk of injury from fragmentation.

- Chain link fencing can be used to reduce the effects of rocket propelled grenades (RPG), as has the use of sandbags to protect bridge wings. Sandbags should be regularly checked to ensure that they have not degraded.

7.4 Control of access to bridge, accommodation and machinery spaces

It is important to deny access to the bridge, accommodation and machinery spaces, to deter or delay attackers who have managed to board a ship and, the following may be considered:

- Escape routes must be easily accessible to seafarers in the event of an emergency. If the door or hatch is locked it is essential that a key is available, in a clearly visible position by the door or hatch.
- All doors and hatches providing access to the bridge, accommodation and machinery spaces should be properly secured to prevent access by attackers.
- It is recommended once doors and hatches are secured, a designated and limited number are used for security patrols and routine access. The use of these doors or hatches should be controlled by the Officer of the Watch.
- Consideration should be given to blocking or lifting external ladders on the accommodation block to prevent use and to restrict external access to the bridge.

- Where doors and hatches must be closed for watertight integrity, clips should be fully dogged down in addition to any locks. Where possible, additional securing, such as with wire strops, may enhance hatch security.
- Removable barriers should be used around pilot boarding points so that a ship does not need to de-rig large areas prior to arrival at ports.

- Attackers can gain access through portholes and windows. The fitting of steel bars to windows will prevent this even if they manage to shatter the glass.
- Procedures for controlling access to accommodation, machinery spaces and store rooms should be briefed to the crew and practiced prior to entering the area of increased risk identified through the risk assessment.

7.5 Physical barriers

Physical barriers should be used to make it as difficult as possible to gain access to ships. Physical barriers offer many options to increase the difficulty of any climb for anyone trying to board the ship.

- Razor wire (also known as barbed tape) creates an effective barrier but only when securely deployed. Selection of appropriate razor wire is important as the quality (wire gauge and frequency of barbs) and type will vary considerably – lower quality razor wire is less effective.

- Concertina razor wire is recommended as the linked spirals make it the most effective barrier.
- Any wire barrier should be constructed of high tensile wire, which is difficult to cut with hand tools. Concertina razor wire coil diameters of between 730 mm or 980 mm are recommended.
- When deploying razor wire personal protective equipment to protect hands, arms and faces should be used. Moving razor wire using wire hooks rather than by hand reduces the risk of injury. It is recommended that razor wire is provided in shorter sections (e.g. 10 m section) as it is significantly easier and safer to use than larger sections which can be very heavy and unwieldy.

- A robust razor wire barrier is particularly effective if it is:
  - Constructed outboard of the ship's structure (i.e. overhanging).
  - Constructed of a double roll of concertina wire – the more rolls the more effective the barrier. The recommended minimum construction is a single high quality roll securely attached outboard of the ship's structure.
  - Properly secured to the ship to prevent attackers from pulling the razor wire off. Consideration should also be given to further securing the razor wire with a wire strop through the razor wire to prevent it being dislodged.
  - Razor wire should be properly maintained so that it does not become rusty. Rusty razor wire is easier to break through.

Depending on the risk assessment, the use of razor wire on the approach to a berth should be rigged as not to interfere with shipboard operations. Chocks and fairleads should be clear, and once alongside if still rigged it should not interfere with port operations; mooring/gangways/loading/discharging. Ships generally maintain the poop area as fully razor wired for the entire period when operating in areas of increased risk identified through the risk assessment.

Other barriers have proven effective – from hanging swinging obstacles over the gunwales to specifically designed overhanging protection which prevents boarding by climbing over the ship's rails.

7.6 Water spray and foam monitors

The use of water spray and/or foam monitors is effective in deterring or delaying any attempt to illegally board a ship. The use of water can make it difficult for an unauthorized boat to remain alongside and makes it significantly more difficult to try to climb aboard. Water spray deterrence should be controlled remotely – manual activation at the hydrant by the crew is unsafe, especially where attackers are using firearms.

- Fire hoses and foam monitors – It is recommended hoses and foam monitors (delivering water) should be fixed in position to cover likely access routes. Improved water coverage may be achieved by using fire hoses in jet mode and utilising baffle plates fixed a short distance in front of the nozzle.
- Water cannons deliver water in a vertical sweeping arc and protect a greater part of the hull.
- Water spray rails – Some ships have installed spray rails using a Glass Reinforced Plastic (GRP) water main, with spray nozzles to produce a water curtain to cover larger areas.
- Foam can be used, but it must be in addition to a ship's standard Fire Fighting Equipment (FFE) stock. Foam is disorientating and very slippery, making it difficult to climb through.

The following points are relevant:

- Once rigged and fixed in position it is recommended hoses and foam monitors are ready to be used, simply requiring remote activation of fire pumps to commence delivery of water.
- Additional power may be required to utilise all pumps; the supporting systems should be ready for immediate use.
- Practice, observation, and drills are required to ensure the equipment provides effective coverage of vulnerable areas.

7.7 Alarms

Sounding the ship's alarm serves to inform the ship's crew an attack is underway. If approached, continuous sounding of the ship's whistle will distract the attackers and let them know that they have been seen. It is important that:

- The alarm is distinctive to avoid confusion with other alarms, potentially leading to the crew mustering at the wrong location.
- Crew members are familiar with each alarm, especially those warning of an attack and indicating "all clear."
- All alarms are backed up by an announcement, in the working language of the ship, over the accommodation and deck PA system.

Drills should be carried out to ensure the alarm is heard throughout the ship. The drill will confirm the time necessary for all personnel to move to a position of safety.

7.8 Manoeuvring practice

Practicing manoeuvring the ship will ensure familiarity with the ship's handling characteristics and how to use avoidance manoeuvres whilst maintaining the best possible speed. Experience has shown that such action can defeat a lengthy and determined pirate attack as creating a wash can have a better defensive impact than speed. Such manoeuvring should only be carried out when it is safe to do so taking into account the navigational situation.

7.9 Closed circuit television

If an attack is underway and attackers are firing at the ship, it is difficult and dangerous to observe whether they have managed to gain access. The use of CCTV coverage can allow the attack to be monitored from a less exposed position:

- Consider the use of CCTV cameras for coverage of vulnerable areas, particularly the poop deck.
- Consider positioning CCTV monitors at the rear of the bridge in a protected position.
- Further CCTV monitors could be located at the safe muster point/citadel.
- Recorded CCTV footage may provide useful evidence after an attack.

7.10 Lighting

Navigation lights should not be switched off at night as this a contravention of international regulations. It is recommended that:

- In areas of increased risk identified through the risk assessment, consideration should be given to the appropriate level of additional lighting to be used.

- Weather deck lighting around the accommodation block and rear facing lighting on the poop deck is available and tested.
- Once attackers have been identified or an attack commences, over side lighting, if fitted, should be switched on. This will dazzle the attackers and give ships staff greater visibility.
- If fitted, search lights should be ready for immediate use.
- At anchor, lights are left on as well-lit ships are less vulnerable to attack.

7.11 Secure storage of ship's tools and equipment

Tools and equipment may be of use to the attackers should be stored in a secure location.

- Ballistic protection to gas bottles or containers of flammable liquids should be considered. Sandbags are not recommended as they degrade quickly if not maintained on a regular basis.
- Excess gas bottles should be landed prior to transit.

7.12 Safe muster points and citadels

When operating in areas area of increased risk identified through the risk assessment careful consideration and detailed planning is critical to the safety and security of the crew. The risk assessment should identify the location of a safe muster point and/or a secure citadel within a ship must also be considered.

7.12.1 Safe muster points

- A safe muster point is a designated area chosen to provide maximum physical protection from attack by pirates and armed robbers to the crew, preferably low down within the

ship. This is where crew not required on the bridge or the engine room control room will muster if the ship is under threat.

- The safe muster point is a short-term safe haven, which will provide protection should the attackers commence firing weapons.
- Select a safe muster point protected by other locked compartments.

7.12.2 Citadels

A citadel is a designated, pre-planned area where, in the event of imminent boarding by attackers, all crew may seek protection. A citadel is designed and constructed to resist forced entry.

Before deciding to use a citadel, thought must be given as to how a citadel situation might end. The use of a citadel cannot guarantee a military or law enforcement response and, the Master may have to make the decision when to end a citadel situation without the assistance of military forces.

Well-constructed citadels used by a well-drilled crew can offer effective protection during an attack. If citadels are used, they must be complementary to, rather than a replacement for, all other SPM.

The establishment of a citadel will require external technical advice and support. However, guidance on construction can be accessed from the sources listed at the annexes and is strongly recommended to be taken into account in the risk assessment.

As well as protection, a citadel must provide reliable means to communicate ashore and maintain some degree of situational awareness. The ability to deny control of propulsion to attackers is a further consideration.

The SSP should define the conditions for use of the citadel and logistics necessary to survive e.g. food, water, medicines, first-aid kits. The use of the citadel must be drilled to ensure the Master is able to make the correct and timely decision on whether to retreat into it.

The whole concept of the citadel approach is lost if any of the crew are left outside before it is secured. Therefore, plans should include a method of ensuring that the entire crew have entered the citadel.

7.13 STS and other static operations

Attackers have boarded ships on STS operations via the fenders.

The use of a chain link fence, particularly if topped with razor wire, attached to the ships side rails and supplemented by stanchions in the vicinity of the fenders provides an effective deterrent to potential boarders. Care must be taken at the interface between the chain link fence and razor wire to ensure that the best possible protection is assured.

The use of gratings, (particularly Glass Reinforced Plastic gratings for ease of fitting) may be secured in way of open Panama or roller fairleads which will further deter any potential boarding.

An additional deterrent in the vicinity of the fenders, and ships fairleads could be the use of water spray.

The hawse pipe should be properly secured to prevent unauthorized access. Use of the anchor wash may also provide a deterrent.

The main engines should be kept at immediate notice so the Master has the option of getting underway in the event of an incident.

Other considerations for the Master during STS or static operations:

- Is there sufficient crew to cover additional security whilst concurrently conducting cargo operations?
- Monitor emails during communications with shore side agents and agencies. Do not activate “reply to all”, since emails may have around twenty (20) addressees. Do not let allow your intentions to be sent to unnecessary and unknown email addresses.

7.14 Unarmed Private Maritime Security Contractors

The use of unarmed private maritime security contractors would be determined by the output of the risk assessment. Consideration should be given to the relevant laws of both flag States and any littoral States. The use of experienced and competent unarmed contractors can be a valuable protective measure, particularly where there may be the requirement to interface and coordinate with local law enforcement agencies, naval forces and coast guards.

7.15 Private Maritime Security Companies (PMSC) and Privately Contracted Armed Security Personnel (PCASP)

The use, of Privately Contracted Armed Security Personnel (PCASP) on board ships would be determined by the out-put of the risk assessment and approval of respective flag State. This guidance does not constitute a recommendation or an endorsement of the general use of PCASP.

Any decision to engage the services of a PMSC & PCASP must be taken after a careful risk assessment of the intended voyage (see section 4) taking into account factors including route, type of cargo, speed, freeboard, and location of any static operations, levels of protection provided by littoral States and the current threat and risk environment. The employment of PCASP is only an additional layer of protection and is not an alternative to other mitigation measures.

The presence on board of PCASPs involves complex legal issues. It is important that permission is obtained from Flag State authorities before PCASP deployment on board. In addition, it is essential to ensure that PCASP are permitted by the governments of all States (littoral States) through whose waters the ship may pass, as the majority of littoral States do not allow PCASP to operate within their territorial waters. Owners must exercise due diligence to check the credentials and licences/permits of the PMSC and where appropriate the PCASPs, to ensure that they are operating legally and that the weapons are also licensed for their use. In addition to firearms, other equipment used by PMSC may be subject to arms control restrictions and also require licences for use by civilians. The owner is under a duty to perform due diligence on the PMSC as the owner will be liable for the PCASP on the ship. It is recommended that shipping companies employ PMSC that are accredited to the ISO 28007 standard (or any future standard that replaces it).

The PMSC must be engaged on a contract such as the BIMCO GUARDCON that does not prejudice the ship's insurance cover arrangements. The contract must be between the company and the PMSC even if the contract price is being paid for or contributed towards by a charterer or other party.

Companies should ensure that the PMSC has insurance policies that are current and compliant with the requirements of the contract.

There must be a clear understanding of the authority of the Master and the Rules for the Use of Force (RUF) under which the PCASP operate. RUF should provide for a graduated, reasonable, proportionate and demonstrably necessary escalation in the application of force in defence of personnel on the ship. The Master always remains the ultimate authority on a ship.

The individual PCASP must always act in accordance with the widely recognised principles of self and collective self-defence.

PCASP procedures should be drilled with the crew to ensure their effectiveness during attack.

This guidance does not constitute a recommendation or an endorsement of the general use of PCASP. The use, or not, of PMSCs and deployment of PCASP on board ships is a decision taken by individual companies following a detailed risk analysis.

If PCASP are deployed on board a ship, this should be included in all reports to designated VRA reporting centres and must be authorised by the flag State. Where risk analysis deems PCASP deployment necessary, it is recommended that companies use PMSC that are accredited to the ISO 28007 standard (or any future standard that replaces it).

If PCASP are to be used they should be as an additional layer of mitigation and protection, not as an alternative to other measures. The crew must not handle or use firearms.

7.16 Vessel Protection Detachments (VPDs)

Armed Vessel Protection Detachments (VPDs) are sometimes deployed on board ships. VPDs consist of armed State-appointed personnel. Their purpose is to deter attackers and, to defend the ship if necessary. The presence on board of VPDs involves complex legal issues and permissions may need to be obtained from the flag State and authorities in coastal and port States.

Action on Attack and/ or Boarding

8.1 General

There are a number of specific actions that may be taken if the crew suspects the ship is under an attack.

A ship could quickly come under attack with little or no warning at any time. This reinforces the need for good lookout, both visual and radar. Attackers using weapons seldom open fire until they are very close to the ship e.g. two cables.

Using whatever time available, no matter how short, to activate any further additional protective measures and plans will make it clear to the attackers that they have been seen, and that the ship is prepared and, will resist attempts to board.

When a ship is at anchor it is unlikely that attackers can be detected and determined as threatening with sufficient warning to enable the ship to get underway and without exposing crew members on the upper deck (particularly the forecastle and bridge wings) to danger.

8.2 Suspicious approach

An approach by small craft may be a prelude to an attack. The Master should be ready to:

- If underway, increase speed and manoeuvre away from the approaching small craft as much as possible to open the distance between the ship and the attackers. Thereafter, steer a straight course to maintain maximum speed. Consider evasive actions if the circumstances dictate and allow.

- Minimise crew movement and confirm the ship's personnel are in a position of safety or warned to be ready to move.
- Activate the ship security alert system (SSAS) which will alert the company and flag state. Put out a distress alert.
- Activate the Emergency Communication Plan.
- Maintain contact with the relevant reporting centre preferably by telephone for as long as it is safe to do so. On receipt of information in relation to an attack, the reporting centre will inform the appropriate national maritime operations/law enforcement centre and in some cases military if in the area, and should ensure all other ships in the immediate vicinity are aware of the event.
- Place the ship's whistle on auto to demonstrate to any potential attacker that the ship is aware of the attack and is reacting to it. Initiate the ship's pre-prepared emergency procedures such as activating water spray and other appropriate self-defence measures.
- Ensure that the Automatic Identification System (AIS) is switched ON.
- Confirm external doors and, where possible, internal public spaces and cabins, are fully secured.

8.3 When under attack

When under attack, the following actions should be taken, as appropriate:

- Make a distress call on VHF and all available means.
- Confirm the attack has been reported to the relevant reporting centre.
- Confirm the SSAS has been activated.
- If underway, commence small alterations of course whilst increasing speed to deter the boarding craft from lying alongside the ship in preparation for boarding. These manoeuvres will create additional wash and make the operation of small craft difficult. To avoid a reduction in speed, large alterations of course are not recommended.
- All crew, except those required on the bridge or in the engine room, move to the safe muster point or citadel. The crew should be given as much protection as possible should the attackers get close enough to use weapons.

8.4 Action if the ship is boarded

If the ship is boarded then the following actions should be taken:

- Stop the engines and take all way off the ship if possible and navigationally safe to do so.
- All remaining crew members to proceed to the citadel or safe muster point. The whole concept of the citadel approach is compromised if any of the crew are left outside before it is secured.
- Ensure all crew are present in the citadel/safe muster point.
- Establish communications with the company and any relevant military/law enforcement authority (see the annexes).

8.5 Action if attackers take control

If attackers take control of the ship, violence or the threat of violence is often used to subdue the crew. The chance of injury or harm is reduced if the crew are compliant and cooperative and the following considered:

- **STOP ALL MOVEMENT WHEN THE ATTACKERS HAVE TAKEN CONTROL AND TRY TO REMAIN CALM.**
- Offer no resistance once the attackers reach the bridge and the crew have not moved to a citadel. The attackers will be aggressive, highly agitated and possibly under the influence of drugs or alcohol. When directed, all movement should be calm, slow, and very deliberate. Crew members should keep their hands visible at all times and comply fully. This will greatly reduce the risk of violence.
- Leave any CCTV or audio recording devices running.
- Do not take photographs.
- DO NOT attempt to confront the attackers.
- DO NOT make movements which could be interpreted as being aggressive.
- DO exactly what they ask and comply with their instruction.

8.6 Kidnap

Kidnap can occur in any region where a threat of piracy and armed robbery exists. Where a ship is hijacked, seafarers may be taken ashore to be held for ransom.

Each company should have a policy in place to cover the eventualities of kidnap and ransom.

The following principles serve as guidelines to seafarers to survive a kidnapping:

DO NOT:

- Be confrontational.
- Offer resistance.
- Take photographs.

DO:

- Be positive.
- Be patient.
- Keep mentally active/occupied.
- Keep track of time.
- Reduce stress where possible by remaining physically active when possible.
- Remain calm and retain dignity.

8.7 In the event of military action

In some areas military or law enforcement action may be provided to assist ships under attack in certain circumstances. On these occasions ship's crew should keep low to the deck and cover their head with both hands, with hands visible. On no account should personnel make movements which could be interpreted as being aggressive:

- Do not take photographs.
- Be prepared to be challenged on your identity. Brief and prepare ship's personnel to expect this and to cooperate fully during any Naval/Military action on board.

Section 9

Post Incident Reporting

9.1 General

Following any attack or suspicious activity, and after initial reporting of the incident, it is vital a detailed report of the incident is made. A copy of the report should be sent to the company, the flag State and other relevant organisations. It is important that any report contains descriptions and distinguishing features of any suspicious vessels that were observed (see the annexes and regional guidance for more detail). This will ensure full analysis and trends in activity of pirates and armed robbers are established and will enable assessment of pirate techniques or changes in tactics, in addition to ensuring appropriate warnings can be issued to other ships in the vicinity.

The period following an attack will be confusing as Companies, Masters and crew recover from the ordeal. To give the investigating authorities the best chance of apprehending the perpetrators it is important that evidence is preserved in the correct manner and, Companies, Masters and crew should refer to IMO Guidelines on Preservation and Collection of Evidence, A28/Res.1091. By following some basic principles, the Master and crew can protect a crime scene until the nominated law enforcement agency arrives. When preserving and collecting evidence, the priority should be:

- Preserve the crime scene and all possible evidence, if passage to a safe harbour is likely to take some time the Master should take initial statements from the crew (this and talking about the event may also help reduce the risk of Post-Traumatic Stress Disorder).
- Avoid contaminating or interfering with all possible evidence – if in doubt, do not touch and leave items in place.
- Do not clean up the area or throw anything away no matter how unimportant it may seem.

- Protect voyage data recorders for future evidence.
- Provide easy access to the crime scene and relevant documentation for law enforcement authorities.

9.2 Investigation

For law enforcement or naval/military forces to hold suspected pirates and armed robbers, following an incident, a witness statement from those affected is required. Seafarers are encouraged to provide witness statements to naval/military forces when requested to do so to enable suspected pirates to be held and handed over to prosecuting states. Without supporting evidence, including witness statements from those affected, suspected attackers are unlikely to be prosecuted.

Law enforcement authorities will routinely request permission to conduct post-release crew debriefs and to collect evidence for on-going and future investigations and prosecutions following captivity. A thorough investigation is critical to ensure that potential physical evidence, including electronic evidence, is not tainted or destroyed or potential witnesses overlooked. The company and crew are advised that the quality of the evidence provided and the availability of the crew to testify will significantly help any investigation or prosecution that follows.

Following any attack or approach the investigating authority will be determined by a number of external factors which may include:

- Coastal State;
- Flag State;
- Ownership;
- Crew nationality.

Regardless of who is appointed the process is generally the same but will be dictated by local law enforcement practice. One overriding principle is that the seafarers should always be treated with respect and as survivors of a crime.

Once appointed, the lead law enforcement agency will talk to the Master and crew to understand the sequence and circumstances of the event. The process used is generally consistent and follows law enforcement practise.

Law enforcement authorities may request permission to conduct post-release crew debriefs and to collect evidence for investigations and prosecutions following captivity. A thorough investigation is critical to ensure that potential physical evidence, including electronic evidence, such as CCTV footage, is not destroyed or potential witnesses overlooked.

The quality of evidence provided and the availability of the crew to testify will significantly help any following investigation or prosecution.

9.3 Reports

It is important a detailed report of the event is provided to the relevant reporting authority. This will enhance knowledge of activity in the maritime domain and better tailor future warnings or advice the regional reporting centres issue to the maritime community.

Companies and Masters may also be required to forward a copy of the completed report to their flag State, and are encouraged to do so.

9.4 Advice

INTERPOL has a dedicated unit for maritime piracy that works with the police, navy, and private sector in member countries, and

can provide support to ship operators who have had their ships hijacked. INTERPOL's Maritime Security sub-Directorate (MTS) can be consulted on the recommended practices and action to be taken to help preserve the integrity of any evidence left behind following a pirate attack that could be useful to law enforcement agents pursuing an investigation.

MTS can be contacted on tel +33 472 44 72 33 or via email dIMTSOPSupport@interpol.int during business hours (GMT 08H00 – 17H00).

Outside of normal business hours, contact can be made via INTERPOL's Command and Co-ordination Centre (CCC). The CCC is staffed 24 hours a day, 365 days a year and supports INTERPOL's 192 member countries faced with a crisis situation or requiring urgent operational assistance. The CCC operates in all four of Interpol's official languages (English, French, Spanish, and Arabic). Contact details are: tel +33 472 44 7676; email os-ccc@interpol.int.

It is recommended that ship operators contact INTERPOL within 3 days of a hijacking of their ship.

Section 10

Humanitarian Considerations

Companies should ensure that seafarers are fully supported after an incident, even one in which an attack has been averted. Seafarers should always be treated with respect and as survivors of crime.

The number to call is +44 207 323 2737. Seafarers should ask for piracy support or for MPHRP by name. SeafarerHelp will contact MPHRP and someone from MPHRP will respond as soon as possible thereafter by calling back.

Further information can be found at http://seafarerswelfare.org/piracy/mphrp.

List of Abbreviations

AIS – Automatic Identification System

BAM – Bab al-Mandeb

CCTV – Closed Circuit Television

CMF – Combined Military Forces

CSO – Company Security Officer

EUNAVFOR – European Naval Forces Operation Atalanta

GoG – Gulf of Guinea

GoO – Gulf of Oman

IFC – Information Fusion Centre Singapore

IMB – International Maritime Bureau

IMB-PRC – International Maritime Bureau Piracy Reporting Centre Kuala Lumpur

IMO – International Maritime Organization

IRTA – Industry Releasable Threat Assessment

IRTB – Industry Releasable Threat Bulletin

ISPS Code – International Ship and Port Facility Security Code

JWC – Lloyd's Joint War Committee

MARSEC Level – Maritime Security Level

MDAT-GOG – Marine Domain Awareness for Trade – Gulf of Guinea

MRCC – Maritime Rescue Coordination Centre

MSCHOA – Maritime Security Horn of Africa

NAVWARN – Navigation Warning

PA System – Public Address System

PCASP – Privately Contracted Armed Security Personnel

PMSC – Private Maritime Security Companies

ReCAAP ISC – Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia

RUF – Rules for the Use of Force

SEA – South East Asia

SPMs – Ship Protection Measures

SSAS – Ship Security Alert System

SSP – Ship Security Plan

STS/SBM – Ship to Ship Transfer/Single Buoy Mooring

UKMTO – United Kingdom Maritime Trade Operations

VHF – Very High Frequency

VPD – Vessel Protection Detachment

VRA – Voluntary Reporting Area

WIO – Western Indian Ocean

Appendix A

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.

3.3 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) on board 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.

Annex A

Western Indian Ocean Region

1. General

This annex covers piracy and armed robbery in the Western Indian Ocean (WIO) region i.e. types of attack and voluntary reporting processes. Admiralty Maritime Security chart Q6099 describes reporting and routing recommendations, and areas of heightened risk.

The geography of the region is diverse and ranges from narrow choke points such as the Bab al-Mandeb (BAM) Straits and the Strait of Hormuz to the wide-open ocean of the Somali basin. Each area presents different challenges and threats will vary.

Attacks on ships and seafarers have taken place throughout the region.

Region-specific guidance for the WIO region is provided in BMP 5.

Joint War Committee Listed Area

The insurance community lists an area of perceived enhanced risk in the region. The geographic limits of all JWC listed areas can be found on their website: www.lmalloyds.com/lma/jointwar.

Maritime Security Transit Corridor

The Maritime Security Transit Corridor (MSTC) is a military established corridor upon which naval forces focus their presence and surveillance efforts. The MSTC is shown on Admiralty Maritime Security chart Q6099.

It is recommended that vessels use the MSTC to benefit from the military presence and surveillance.

2. Industry Releasable Threat Assessments and Bulletins

EUNAVFOR and CMF produce regular Industry Releasable Threat Assessments (IRTA) to inform risk management decision making for companies operating merchant ships transiting through the Red Sea, Gulf of Aden (GoA), Gulf of Oman (GoO) and the Western Indian Ocean. The IRTAs are complimented by Industry Releasable Threat Bulletins (IRTB), also produced by EUNAVFOR and CMF, which cover specific events and reflect the dynamic nature of the operating environment. They are a vital resource to ensure the safety of ships in the region, and should be fully considered as part of the risk assessment.

3. Registration and Reporting

UKMTO is the first point of contact for ships in the region. The day-to day interface between Masters and naval/military forces is provided by UKMTO, which tallks to merchant ships and liaises directly with MSCHOA and naval commanders at sea and ashore. Merhcant ships are strongly encouraged to regularly send reports to UKMTO.

MSCHOA is the planning and coordination centre for EU Naval Forces (EUNAVFOR) MSCHOA encourages companies to register their ship's movements before entering the HRA and if participating in the group transit system via their website www.mschoa.org.

The MSCHOA and UKMTO voluntary registration and reporting scheme in the WIO has proven extremely effective. It is important that reporting procedures are followed in order for military forces to monitor and give guidance at short notice on threats in the region. Ship reporting is the major indicator to MSCHOA on the level of implementation of protective measures.

Regional Contacts:

UKMTO (United Kingdom Maritime Trade Operations)

Email: watchkeepers@ukmto.org
Tel: +44 2392 222060
+971 50 552 3215
Web: www.ukmto.org

MSCHOA

Email: postmaster@mschoa.org
Tel: +44 (0)1923 958 545
+44 (0)1923 958 700
Fax: +44 (0)1923 958 520
Web: www.mschoa.org

USN Naval Control and Guidance to Shipping

Email: cusnc.ncags_bw@me.navy.mil
Tel: +973 3905 9583 (24hr duty phone)
Office: +973 1785 1023 (Office)

Other Useful Contacts

IMB Piracy Reporting Centre (IMB PRC)

Email: piracy@icc-ccs.org
Tel: +60 3 2031 0014
Fax: +60 3 2078 5769
Web: www.icc-ccs.org/piracy-reporting-centre/live-piracy-map

Further Information

Further information and guidance can be obtained from the following organisations, websites or publications:

- IMO Maritime Safety Committee Circulars.
- Annual Summary of Admiralty Notices to Mariners.
- Admiralty List of Radio Signals (ALRS) volumes 1 and 6.
- The Mariner's Handbook, Chapter 13.
- Relevant Navigation Warnings and EGC SafetyNet broadcasts on Inmarsat C.

Annex B

Gulf of Guinea Region

1. General

This annex covers the Gulf of Guinea (GoG) Region, types of attack and voluntary reporting processes. The area off the coasts of Cameroon, Benin Ghana, Nigeria and Togo, can be regarded as that in which mitigation measures against piracy and armed robbery should be applied. Attacks have occurred from as far south as Angola and north as Sierra Leone.

Region-specific guidance for the GoG region is provided in Guidelines for Owners Operators and Masters for Protection against piracy and armed robbery in the Gulf of Guinea Region.

Joint War Risk Listed Area

Lloyds JWC has designated an area as being of perceived enhanced risk, and the JWC Listed areas should be consulted within a risk assessment to determine the appropriate self-protective measures that should be applied.

Registration and Reporting

The MDAT-GOG is the first point of contact for ships in the region offering a voluntary registration and reporting scheme. Merchant ships are strongly encouraged to register and report as highlighted in regional guidance and Chart Q6114 and French Navy Hydrographic Chart SHOM 8801CS.

MDAT-GoG

Tel: +33(0)2 98 22 88 88

Email: watchkeepers@mdat-gog.org

Other Useful Contacts

IMB Piracy Reporting Centre (IMB PRC)

Tel: +60 3 2031 0014
Fax: +60 3 2078 5769
Email: piracy@icc-ccs.org
Web: www.icc-ccs.org/piracy-reporting-centre/live-piracy-map

Annex C

Asian Region

1. General

Acts of piracy and armed robbery have occurred in the straits of Malacca and Singapore, the southern portion of the South China Sea, the Sulu-Celebes Seas and at certain ports and anchorages in Asia.

Region-specific guidance for the Asian region is provided in Regional Guide to Counter Piracy and Armed Robbery against Ships in Asia.

Reporting

The Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) is the first regional government-to-government agreement to promote and enhance cooperation against piracy and armed robbery in Asia. Under the Agreement, the ReCAAP Information Sharing Centre (ReCAAP ISC) was launched in Singapore in November 2006. It was formally recognized as an international organization in January 2007. To date, 20 States have become Contracting Parties to ReCAAP.

Under the Agreement, Coastal States undertake the ownership to suppress piracy and armed robbery against ships, thus the reporting of incidents is based on this principle. The ReCAAP ISC strongly recommends the victim ship to report immediately the incident to the nearest Coastal State through its MRCC, in accordance with the IMO/MSC Circular 1334. The Coastal State is urged to undertake appropriate response. ReCAAP Focal Point of the Coastal State shares the verified information of incident through the Information Network System with the ReCAAP ISC and other Focal Points on a 24/7 basis. Based on the verified information, the ReCAAP ISC issues a warning and/or an alert, as appropriate.

The Information Fusion Centre (IFC) is a multi-national maritime security information centre based in Singapore. It has international liaison officers from the of more than 10 countries working at the

centre. The IFC aims to achieve early warning of maritime security threats through information-sharing cooperation with its partners to facilitate timely operational responses. Best Management Practice should be followed where practicable, taking into account inputs from the local maritime security agencies.

The Singapore IFC voluntary registration and reporting scheme is well established. This VRA is extremely large and should be considered in conjunction with the IFC listed 'areas of concern' and guidance provided when preparing a risk assessment. In the event of a suspicious approach or an actual attack, the Master should contact the nearest coastal State through its MRCC. Reporting requirements in Asia are complex and full details are contained in the Admiralty Charts Q6112 and Q6113.

Regional Contacts

Information Fusion Centre (IFC)

Email: information_fusion_centre@defence.gov.sg
Tel: +65 6594 5728 or +65 9626 8965
Fax: +65 6594 5734
Web: www.infofusioncentre.gov.sg

ReCAAP Information Sharing Centre

Email: info@recaap.org
Tel: +65 6376 3063
Fax: +65 6376 3066
Web: www.recaap.org

IMB Piracy Reporting Centre (IMB PRC)

Email: piracy@icc-ccs.org
Tel: +60 3 2031 0014
Fax: +60 3 2078 5769
Web: www.icc-ccs.org/piracy-reporting-centre/live-piracy-map

Supporting Organisations

BIMCO

BIMCO is the world's largest international shipping association, with around 2,000 members in more than 120 countries, representing 56% of the worlds tonnage. Our global membership includes shipowners, operators, managers, brokers and agents. A non-profit organisation, BIMCO's mission is to be at the forefront of global developments in shipping, providing expert knowledge and practical advice to safeguard and add value to members' businesses.

The Chemical Distribution Institute

CDI was established in 1994 as a not for profit Foundation and provides ship and terminal inspection data in an electronic report format to its members. The main objectives of CDI is to continuously improve the safety and quality performance of chemical marine transportation and storage; Through cooperation with industry and centres of education, drive the development of industry best practice in marine transportation and storage of chemical products; To provide information and advice on industry best practice and international legislation for marine transportation and storage of chemical products; To provide chemical companies with cost effective systems for risk assessment, thus assisting their commitment to Responsible Care and the Code of Distribution Management Practice.

www.cdi.org.uk

Cruise Lines International Association (CLIA)

CLIA is the world's largest cruise industry trade association, providing a unified voice and leading authority of the global cruise community. CLIA supports policies and practices that foster a safe, secure, healthy and sustainable cruise ship environment for the more than 25 million passengers who cruise annually and is dedicated to promote the cruise travel experience. The organization's mission is to be the unified global organization that helps its members succeed by advocating, educating and promoting for the common interests of the cruise community.

International Chamber of Shipping (ICS)

International Chamber of Shipping
Shaping the Future of Shipping

ICS is the international trade association for merchant ship operators. ICS represents the collective views of the international industry from different nations, sectors and trades. ICS membership comprises national shipowners' associations representing over 80% of the world's merchant fleet. A major focus of ICS activity is the International Maritime Organization (IMO), the United Nations agency with responsibility for the safety of life at sea and the protection of the marine environment. ICS is heavily involved in a wide variety of areas including any technical, legal and operational matters affecting merchant ships. ICS is unique in that it represents the global interests of all the different trades in the industry: bulk carrier, tanker, container, and passenger ship operators.

www.ics-shipping.org

The International Association of Dry Cargo Shipowners (INTERCARGO)

INTERCARGO, established in 1980 in London and granted IMO NGO consultative status since 1993, is a voluntary non-profit association representing the interests of dry cargo vessel owners.

INTERCARGO provides the forum where quality dry bulk shipowners, managers and operators are informed about, discuss and share concerns on key topics and regulatory challenges, especially in relation to safety, the environment and operational excellence.

INTERCARGO promotes best practices and represents dry cargo shipping interests at IMO, other industry fora and the broader business context, basing its strategies on the principle of free and fair competition.

International Federation of Shipmasters' Associations (IFSMA)

IFSMA was formed in 1974 by Eight National Shipmasters' Associations to unite the World's serving Shipmasters into a single professional co-ordinated body. It is a non-profit making apolitical organisation dedicated solely to the interest of the serving Shipmaster. The Federation is formed of around 11,000 Shipmasters from sixty Countries either through their National Associations or as Individual Members. In 1975, IFSMA was granted Consultative Status as a non-governmental organisation at IMO which enables the Federation to represent the views and protect the interests of the serving Shipmasters.

International Group of P&I Clubs

Thirteen principal underwriting associations "the Clubs" comprise the International Group. They provide liability cover (protection and indemnity) for approximately 90% of the world's ocean-going tonnage. The Clubs are mutual insurance associations providing cover for their members against third party liabilities relating to the use and operation of ships, including loss of life, pollution by oil and hazardous substances, wreck removal, collision and damage to property. Clubs also provide services to their members on claims handling, legal issues and loss prevention, and often play a leading role in coordinating the response to, and management of, maritime casualties.

International Marine Contractors Association (IMCA)

IMCA represents the vast majority of offshore marine contractors and the associated supply chain in the world, with members from over 60 countries. It publishes an extensive technical library of guidance documents on operational good practice, safety promotional materials, timely information notes and safety flashes. Its members benefit from a technical structure comprising four main divisions covering Offshore Diving, Marine, Remote Systems and ROVs, and Offshore Surveying.

These are supported by a committee structure focused on: health, safety, security and the environment; competence and training; lifting and rigging; marine policy and regulatory affairs; and contracts and insurance. The Association's global coverage is organised into five geographic regions: Asia-Pacific, Europe & Africa, Middle East & India, North America, and South America.

InterManager

InterManager is the international trade association for the ship management industry. Our members are in-house or third party ship managers, crew managers or related organisations and related maritime businesses and organisations. Collectively InterManager members are involved in the management of more than 5,000 ships and responsible for in excess of 250,000 seafarers.

International Maritime Bureau

Established in 1992, IMB Piracy Reporting Centre (IMB PRC) provides the shipping industry with a free 24-hour service to report any piracy or armed robbery incidents occurring anywhere in the world.

The IMB PRC is an independent and non-governmental agency aimed at raising awareness of areas at risk of these attacks. As a trusted point of contact for shipmasters reporting incident to the IMB PRC from anywhere in the world, the IMB PRC immediately relays all incidents to the local law enforcement requesting assistance. Information is also immediately broadcast to all vessels via Inmarsat Safety Net to provide and increase awareness.

www.icc-ccs.org/piracy-reporting-centre

The International Parcel Tankers Association (IPTA)

IPTA was formed in 1987 to represent the interests of the specialised chemical/parcel tanker fleet and has since developed into an established representative body for ship owners operating IMO classified chemical/parcel tankers, being recognised as a focal

point through which regulatory authorities and trade organisations may liaise with such owners. IPTA was granted consultative status as a Non-Governmental Organisation to the International Maritime Organization (IMO) in 1997 and is wholly supportive of the IMO as the only body to introduce and monitor compliance with international maritime legislation.

www.ipta.org.uk

International Maritime Employers' Council Ltd (IMEC)

IMEC is the only international employers' organisation dedicated to maritime industrial relations. With offices in the UK and the Philippines, IMEC has a membership of over 235 shipowners and managers, covering some 8,000 ships with CBA's, which IMEC negotiates on behalf of its members within the International Bargaining Forum (IBF).

IMEC is also heavily involved in maritime training. The IMEC Enhanced cadet programme in the Philippines currently has over 700 young people under training.

The International Seafarers Welfare and Assistance Network (ISWAN)

ISWAN is an international NGO and UK registered charity set up to promote the welfare of seafarers worldwide. We are a membership organisation with ship owners, unions and welfare organisation as members. We work with a range of bodies including P&I Clubs, shipping companies, ports, and governments. Our focus is the wellbeing of the 1.5 million seafarers around the world.

We support seafarers and their families who are affected by piracy and our 24-hour multilingual helpline, SeafarerHelp, is free for seafarers to call from anywhere in the world.

www.seafarerswelfare.org

International Transport Workers' Federation (ITF)

ITF is an international trade union federation of transport workers' unions. Any independent trade union with members in the transport industry is eligible for membership of the ITF. The ITF has been helping seafarers since 1896 and today represents the interests of seafarers worldwide, of whom over 880,000 are members of ITF affiliated unions. The ITF is working to improve conditions for seafarers of all nationalities and to ensure adequate regulation of the shipping industry to protect the interests and rights of the workers. The ITF helps crews regardless of their nationality or the flag of their ship.

www.itfseafarers.org
www.itfglobal.org

INTERTANKO

INTERTANKO is the International Association of Independent Tanker Owners, a forum where industry meets, policies are discussed and best practices developed. INTERTANKO has been the voice of independent tanker owners since 1970, ensuring that the liquid energy that keeps the world turning is shipped safely, responsibly and competitively.

www.intertanko.com

Joint War and Hull Committees

The Joint Hull and Joint War Committees comprise elected underwriting representatives from both the Lloyd's and IUA company markets, representing the interests of those who write marine hull and war business in the London market.

Both sets of underwriters are impacted by piracy issues and support the mitigation of the exposures they face through the owners' use of BMP. The actions of owners and charterers will inform underwriters' approach to risk and coverage.

http://www.lmalloyds.com/lma/jointhull
http://www.lmalloyds.com/lma/jointwar

The Oil Companies International Marine Forum (OCIMF)

OCIMF is a voluntary association of oil companies (the 'members') who have an interest in the shipment and terminalling of crude oil, oil products, petrochemicals and gas. OCIMF's mission is to be the foremost authority on the safe and environmentally responsible operation of oil tankers, terminals and offshore support vessels, promoting continuous improvement in standards of design and operation.

www.ocimf.org

The Society of Independent Gas Tanker and Terminal Operators Ltd (SIGTTO)

The Society is the international body established for the exchange of technical information and experience, between members of the industry, to enhance the safety and operational reliability of gas tankers and terminals.

To this end the Society publishes studies, and produces information papers and works of reference, for the guidance of industry members. It maintains working relationships with other industry bodies, governmental and intergovernmental agencies, including the International Maritime Organization, to better promote the safety and integrity of gas transportation and storage schemes.

http://www.sigtto.org

The World Shipping Council (WSC)

WSC is the trade association that represents the international liner shipping industry. WSC's member lines operate containerships, roll-on/roll-off vessels, and car carrier vessels that account for approximately 90 percent of the global liner vessel capacity. Collectively, these services transport about 60 percent of the value of global seaborne trade, or more than US$ 4 trillion worth of goods annually. WSC's goal is to provide a coordinated voice for the liner shipping industry in its work with policymakers and other industry groups to develop actionable solutions for some of the world's most challenging transportation problems. WSC serves as a non-governmental organization at the International Maritime Organization (IMO).

www.worldshipping.org

Supporting Naval/ Military Forces/ Law Enforcement Organisations

Combined Maritime Forces (CMF)

CMF is an enduring global maritime partnership of 32 willing nations aligned in common purpose to conduct Maritime Security Operations (MSO) in order to provide security and stability in the maritime environment. CMF operates three Combined Task Forces (CTF) across the Red Sea, Gulf of Aden, Somali Basin, Northern Arabian Sea, Gulf of Oman, Indian Ocean and the Arabian Gulf. CTF150 is responsible for maritime security and counter-terrorism, CTF151 is responsible for deterring, disrupting and suppressing piracy and CTF152 is responsible for maritime security and counter-terrorism specifically in the Arabian Gulf. Visit www.combinedmaritimeforces.com or e-mail us at cmf_info@me.navy.mil

EUNAVFOR (The European Naval Force)

Piracy and other maritime security issues have continued to be a threat to mariners who transit the Southern Rea Sea, Horn of Africa and the Western Indian Ocean. The mission of EU NAVFOR is (1) to PROTECT World Food Programme and other vulnerable shipping and (2) to deter, prevent and repress acts of piracy and armed robbery at sea. This requires (3) the enhancement of cooperation and coordination with an increasingly wide range of

maritime actors to uphold freedom of navigation across a broad maritime security architecture. EU NAVFOR is also tasked with (4) monitoring fishing activities off the coast of Somalia. Thus, acting as a catalyst for action, EU NAVFOR continues to promote solutions to regional maritime security issues, thereby contributing to the EU's much wider security, capacity-building and capability-building work in this strategically important location.

http://eunavfor.eu/

INTERPOL

INTERPOL has a dedicated unit for maritime piracy that works with the police, navy, and private sector in member countries, and can provide support to ship operators who have had their ships hijacked. INTERPOL's Maritime Security sub-Directorate (MTS) can be consulted on the recommended practices and action to be taken to help preserve the integrity of any evidence left behind following a pirate attack that could be useful to law enforcement agents pursuing an investigation.

MTS can be contacted on tel +33 472 44 72 33 or via email dIMTSOPSupport@interpol.int during business hours (GMT 08H00 – 17H00).

Outside of normal business hours, contact can be made via INTERPOL's Command and Co-ordination Centre (CCC). The CCC is staffed 24 hours a day, 365 days a year and supports INTERPOL's 192 member countries faced with a crisis situation or requiring urgent operational assistance. The CCC operates in all four of Interpol's official languages (English, French, Spanish, and Arabic). Contact details are: tel +33 472 44 7676; email os-ccc@interpol.int

It is recommended that ship operators contact INTERPOL within 3 days of a hijacking of their ship.

Maritime Security Centre Horn of Africa (MSCHOA)

MSCHOA is an integral part of EU NAVFOR, sitting functionally within the Operational Headquarters and staffed by military and civilian EU NAVFOR personnel. The MSCHOA provides a service to mariners in the Gulf of Aden, the Somali Basin and off the Horn of Africa. It is a Coordination Centre dedicated to safeguarding legitimate freedom of navigation in light of the risk of attack against merchant shipping in the region, in support of the UN Security Council's Resolutions (UNSCR) 1816 and subsequent reviews. EU NAVFOR and CMF are committed to ensuring that mariners have the most up to date regular threat assessments and incident specific bulletins, published by the MSCHOA. Through close dialogue with shipping companies, ships' masters and other interested parties, MSCHOA builds up a picture of vulnerable shipping in these waters and their approaches. The MSCHOA can then act as a focal point sharing information to provide support and protection to maritime traffic. There is a clear need to protect ships and their crews from illegitimate and dangerous attacks, safeguarding a key global trade route.

www.mschoa.org

UK Maritime Trade Operations (UKMTO)

UKMTO capability acts as the primary point of contact for merchant vessels and liaison with military forces within the region. UKTMO also administers the Voluntary Reporting Scheme, under which merchant vessels are encouraged to send regular reports, providing their position/speed and ETA at the next port of call, in accordance with the Maritime Security Chart Q6099.

Emerging and time relevant information impacting commercial traffic can then be passed directly to vessels at sea, and responding assets accordingly, therefore improving the collective responsiveness to an incident. For further information on UKTMO please contact:

Emergency Telephone Numbers:
+44 (0)2392 222060 or +971 5055 23215
Email: watchkeepers@ukmto.org
Web: www.ukmto.org

Witherby Publishing Group
www.witherbys.com