INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC.1/Circ.1601
7 December 2018

REVISED INDUSTRY COUNTER PIRACY GUIDANCE

1 The Maritime Safety Committee, at its eighty-ninth session (11 to 20 May 2011) having, inter alia, recognized the importance of the Best Management Practices (BMP) and the need to comply with the provisions therein, adopted resolution MSC.324(89) on *Implementation of Best Management Practice Guidance*, and expressed its general understanding of the need to keep the BMP alive, relevant, dynamic and updated.

2 The Committee noted that the industry group was working on a revision to the Best Management Practices to Deter Piracy off the Coast of Somalia and in the Arabian Sea Area. The Committee therefore authorized the Chair and the Secretariat to distribute the revised Best Management Practices guidance without waiting for the Committee's prior approval and subsequently endorsed MSC.1/Cirlc.1339 retrospectively at its ninetieth session (16 to 25 May 2012).

3 At its 100th session (3 to 7 December 2018), the Committee noted that the shipping industry had comprehensively reviewed and updated its guidance on piracy and armed robbery, resulting in the development of Global Counter Piracy Guidance for Companies, Masters and Seafarers; the revised Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea (BMP5); the guidelines for protection against piracy and armed robbery in the Gulf of Guinea region (Version 3); and the launch of a dedicated security website: www.maritimeglobalsecurity.org

4 The Committee further noted that the new and revised guidance takes into account developments in piracy and maritime security since the publication of BMP4, including the development of further regional guidance, changes in pirate modus operandi and the establishment of new regional reporting mechanisms. The guidance is publically available and is intended to assist companies and seafarers to further mitigate maritime security threats, and help increase the security of world trade. Consequently, the Committee approved the *Revised Industry Counter Piracy Guidance* set out in the annexes.

5 Member Governments are invited to take note of the Global Counter Piracy Guidance for Companies, Masters and Seafarers, as set out in annex 1; the revised Best Management Practices (BMP5), as set out in annex 2; and protection against piracy and armed robbery in the Gulf of Guinea region as set out in annex 3; and advise owners, operators and managers of ships entitled to fly their flag, as well as the shipboard personnel employed or engaged on such ships, to act accordingly.

IMO 70 OUR HERITAGE BETTER SHIPPING FOR A BETTER FUTURE

6 The Guidance provided in annex 1 is intended to support existing IMO guidance, namely the *Recommendations to Governments for preventing and suppressing piracy and armed robbery against ships* (MSC.1/Circ. 1333/Rev.1), the *Guidance to shipowners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships* (MSC.1/Circ.1334) and resolution MSC.324(89) on *Implementation of Best Management Practice Guidance*, and is complementary to regional initiatives which provide more detailed guidance specific to the threat in a particular region.

7 International organizations are also invited to take note of the Guidance and to advise their membership to act accordingly.

8 Member Governments and international organizations are invited to consider bringing the results of the experience gained with the application of this guidance to the attention of the Committee.

9 This circular revokes MSC.1/Circ.1339.

***

ANNEX 1

Global Counter Piracy Guidance for Companies, Masters and Seafarers

Produced and supported by:

BIMCO · CDI · CLIR · 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 · INTERPOL · MARITIME SECURITY CENTRE · 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

Legal Notice
This Global Counter Piracy Guidance for Companies, Masters and Seafarers has been developed purely as guidance to be used at the user's own risk. No responsibility is accepted by the Authors, their Members or by any person, firm, corporation or organisation for the accuracy of any information in this Guidance or any omission from this Guidance or for any consequence whatsoever resulting directly or indirectly from applying or relying on this Guidance even if caused by a failure to exercise reasonable care.

Copyright Notice
The Authors of this Guidance have provided the Guidance free of charge. All information, data and text contained in this Guidance whether in whole or in part may be reproduced or copied without any payment, individual application or written license provided that:

- It is used only for non-commercial purposes; and
- the content is not modified.

Exceptions:
The permission granted above permits the photographs to be used within the whole or part of this Guidance. The permission does not extend to using the photographs separately outside of this Guidance as these photographs belong to a third party. Authorisation to use the photographs separately from this Guidance must first be obtained from the copyright holders, details of whom may be obtained from the Authors.

The diagram "Limits of Maritime Security Charts" on page 4 is subject to Crown Copyright and/or database rights and is reproduced by permission of the Controller of Her Majesty's Stationery Office and the UK Hydrographic Office (www.GOV.uk/UKHO).

Logos and trademarks are excluded from the general permission above other than when they are used as an integral part of this Guidance.

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		v
Aide Memoire		vi
Section 1	Introduction	1
Section 2	Piracy and Armed Robbery against Ships Worldwide	4
Section 3	Voluntary Reporting	7
Section 4	Company Threat and Risk Assessment	9
Section 5	Company Planning	12
Section 6	Ship Master's Planning	15
Section 7	Ship Protection Measures (SPM)	22
Section 8	Action on Attack and/or Boarding	40
Section 9	Post Incident Reporting	45
Section 10	Humanitarian Considerations	49
List of Abbreviations		50
Appendix A	Other Maritime Security Threats	52
Annex A	Western Indian Ocean Region	57

Annex B **Gulf of Guinea Region** **61**

Annex C **Asian Region** **63**

Supporting Organisations **65**

Supporting Naval/Military Forces/ Law Enforcement Organisations **74**

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.

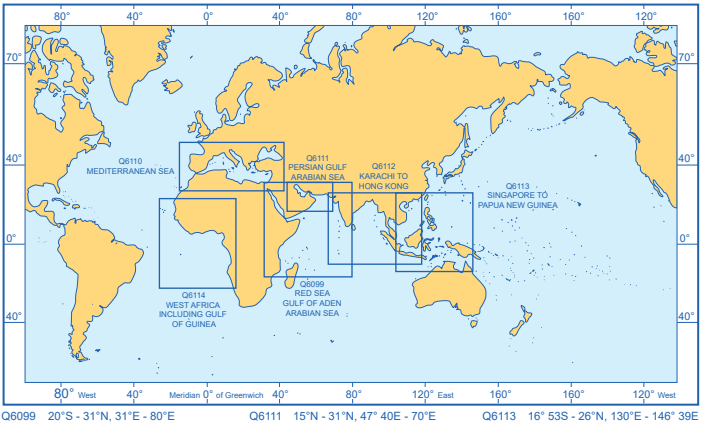
Piracy and Armed Robbery against Ships Worldwide

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)

LIMITS OF MARITIME SECURITY CHARTS



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

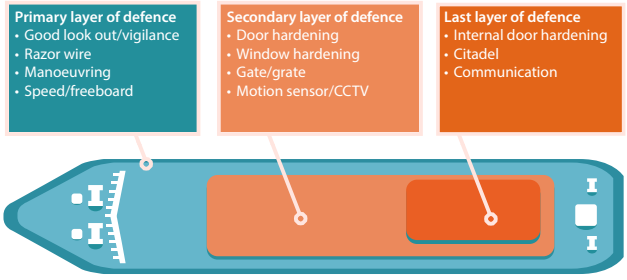
This section focuses on measures that can be taken by the ship's crew to mitigate against attack.

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.

5.5 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.

5.6 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.

5.7 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

Joint War Committee

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

ANNEX 2

BMP5

Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea

Produced and supported by:

BIMCO · CDI · CLIR · International Chamber of Shipping · IFSMA · IGP&I International Group of P&I Clubs · IMCA · INTERCARGO · InterManager · IMEC · INTERTANKO · IPTA International Parcel Tankers Association · ISWAN · Joint Hull committee · Joint War Committee · The Mission to Seafarers · OCIMF · Sailors' Society · SIGTTO · World Shipping Council · Contact Group on Piracy off the Coast of Somalia · EU NAVFOR Somalia · Maritime Security Centre · ICC International Maritime Bureau · Information Fusion Centre · INTERPOL · Royal Navy

ANNEX 2

BMP5

Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea

ANNEX 2

Version 5 published June 2018

Authors: BIMCO, ICS, IGP&I Clubs, INTERTANKO and OCIMF

Legal Notice

BMP5 has been developed purely as guidance to be used at the user's own risk. No responsibility is accepted by the Authors, their Members or by any person, firm, corporation or organisation for the accuracy of any information in BMP5 or any omission from BMP5 or for any consequence whatsoever resulting directly or indirectly from applying or relying upon guidance contained in BMP5 even if caused by a failure to exercise reasonable care.

Copyright notice

The Authors of BMP5 have provided BMP5 free of charge. All information, data and text contained in BMP5 whether in whole or in part may be reproduced or copied without any payment, individual application or written license provided that:

- It is used only for non-commercial purposes; and
- The content is not modified

Exceptions:

The permission granted above permits the photographs to be used within the whole or part of BMP5. The permission does not extend to using the photographs separately outside of BMP5 as these photographs belong to a third party. Authorisation to use the photographs separately from BMP5 must first be obtained from the copyright holders, details of whom may be obtained from the Authors.

Logos and trademarks are excluded from the general permission above other than when they are used as an integral part of BMP5.

Published by

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

Tel No: +44 (0) 1506 463 227
Fax No: +44 (0) 1506 468 999
Email: info@emailws.com
Web: www.witherbys.com

Contents

The fundamental requirements of BMP		iv
Section 1	Introduction	1
Section 2	The threat	4
Section 3	Threat and risk assessment	6
Section 4	Planning	8
Section 5	Ship Protection Measures	11
Section 6	Reporting	21
Section 7	Ships under attack	23
Annex A	Contact details	33
Annex B	Maritime security charts	35
Annex C	Common understanding	36
Annex D	UKMTO reporting forms	38
Annex E	Maritime Security Centre – Horn of Africa reporting forms	40
Annex F	Additional guidance for vessels engaged in fishing	47
Annex G	Additional advice for leisure craft, including yachts	49
Annex H	Definitions and abbreviations	50
Annex I	Supporting organisations	53
Annex J	Voyage reference card	69

ANNEX 2

The fundamental requirements of BMP

Understand the threat

- Maritime threats are dynamic.
- Obtaining current threat information is critical for risk assessment and decision making.

Conduct risk assessments

- Companies must conduct risk assessments.
- Identify ship protection measures.

Implement ship protection measures

- Harden the ship.
- Brief and train the crew.
- Enhanced lookout.
- Follow Flag State and military guidance.

Report

- Report to UKMTO and register with MSCHOA.
- Report incidents and suspicious activity.
- Send distress signal when attacked.

Cooperate

- Cooperate with other shipping and military forces.
- Cooperate with law enforcement to preserve evidence.
- Cooperate with welfare providers.

Section 1

Introduction

Seafarers have encountered different security threats when operating ships in the Red Sea, the Gulf of Aden, the Indian Ocean and the Arabian Sea.

The purpose of this publication is to help ships plan their voyage and to detect, avoid, deter, delay and report attacks. Experience has shown application of the recommendations in this publication makes a significant difference to the safety of seafarers.

Piracy-specific Best Management Practice (BMP), international navies and capacity building ashore have helped to suppress piracy. However, Somali piracy has not been eradicated and remains a threat.

The BMP contained in this publication mitigates the risk from piracy and other maritime security threats.

Regional instability has introduced other maritime security threats, which include:

- Deliberate targeting of ships by extremist groups.
- Collateral damage arising from regional conflict.

BMP piracy measures are effective, but differences in attack methods from other threats may require other forms of mitigation. For example, attacks carried out by extremists may be more determined, as they may be willing to risk their lives.

The consequences of not adopting effective security measures can be severe. Some pirates have subjected hostages to violence and other ill treatment and periods of captivity for some hijacked seafarers have lasted for several years. Other attacks have demonstrated an intent to damage ships and endanger life.

The United Kingdom Maritime Trade Operations (**www.ukmto.org**) and Maritime Security Centre – Horn of Africa (**www.mschoa.org**) websites should be consulted for advice. See annex A for contact details.

This BMP complements piracy guidance in the latest International Maritime Organization (IMO) MSC Circulars (see **www.imo.org**) and advice on the Maritime Security Transit Corridor.

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

Geographical area

The geography of the region is diverse and ranges from narrow choke points such as the Bab el 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. Threats are dynamic; information should be sought from the organisations listed in annex A.

Voluntary Reporting Area

The UKMTO Voluntary Reporting Area (VRA) is identified on maritime security charts such as UKHO Q6099. Ships entering and operating within the VRA are encouraged to register with the UKMTO. Registration establishes direct contact between the reporting ship and UKMTO.

MSCHOA vessel registration area

The MSCHOA vessel registration area is designed to inform military counter piracy forces of the transit of merchant ships in the Indian Ocean and the Gulf of Aden. The MSCHOA vessel registration area is defined on maritime security chart Q6099.

High Risk Area

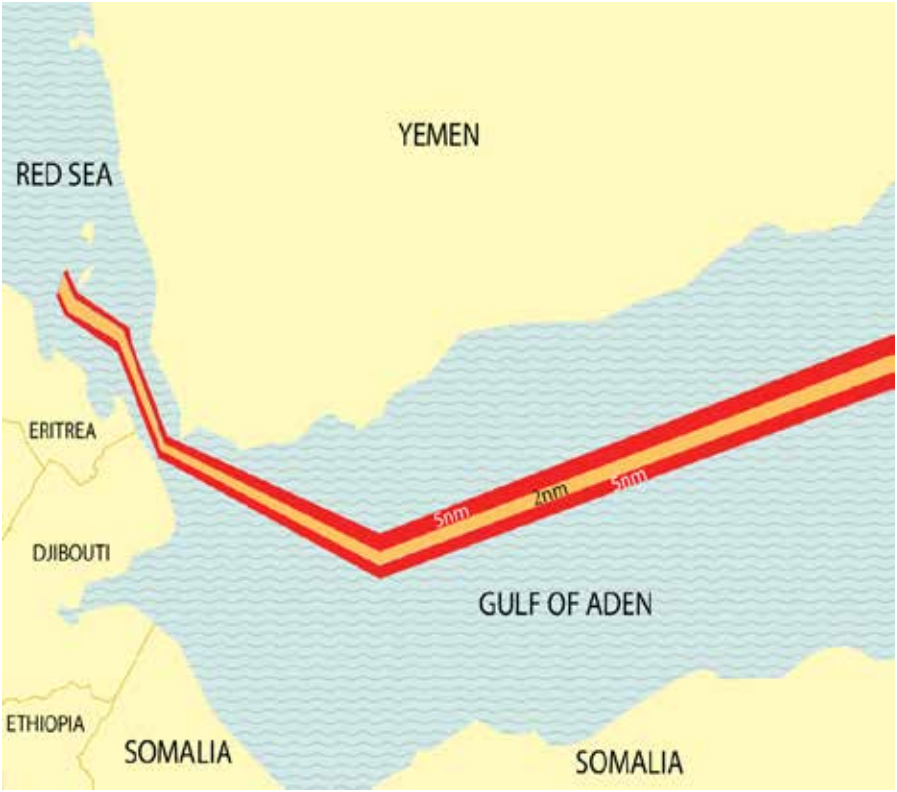
A High Risk Area (HRA) is an industry defined area within the VRA where it is considered that a higher risk of attack exists, and additional security requirements may be necessary. The HRA is outlined on maritime security chart Q6099. It is important the latest information on current threats is used when planning routes through the HRA. Ships should be prepared to deviate from their planned route at short notice to avoid threats highlighted by navigation warnings or by military forces.

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 maritime security chart Q6099 and the figure below and consists of:

- The Internationally Recommended Transit Corridor (IRTC).
    - The IRTC is not a Traffic Separation Scheme (TSS) but an established transit corridor in the Gulf of Aden where naval forces focus their counter piracy patrols. Within the IRTC, group transits and national convoys may be offered.
- The BAM TSS and the TSS West of the Hanish Islands.
- A two-way route directly connecting the IRTC and the BAM TSS.

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



Joint War Committee listed area

The insurance community may list 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 the JWC listed area can be found on their website: **www.lmalloyds.com/lma/jointwar**.

Section 2

The threat

As well as piracy, regional instability has introduced new security threats including the use of:

- Anti-ship missiles.
- Sea mines.
- Water-Borne Improvised Explosive Devices (WBIED).

Piracy

Pirates operate in Pirate Action Groups (PAG) who operate several different boat configurations, typically using small high speed (up to 25 knots) open boats or skiffs.

PAG boat configurations include:

- Skiffs only.
- Open whalers carrying significant quantities of fuel and often towing one or more attack skiffs.
- Motherships, which include merchant ships and fishing vessels but, more commonly, dhows.

Where motherships are used the crew are often held onboard as hostages. Motherships are used to carry pirates, stores, fuel and attack skiffs to enable pirates to operate over a much larger area and are significantly less affected by the weather. Attack skiffs are often towed behind motherships. Where the size of the mothership allows, skiffs may be carried onboard and camouflaged.

Pirates may use small arms fire and Rocket Propelled Grenades (RPGs) to intimidate Masters of ships to reduce speed or stop to allow them to board. The bridge and accommodation tend to be the main targets for these weapons.

Pirates use long lightweight ladders, knotted climbing ropes or long hooked poles to climb up the side of the ship. Once onboard they will make their way to the bridge to try to take control of the ship. When on the bridge they will demand the ship slows/stops to enable other pirates to board.

Attacks can take place at any time – day or night – however experience shows attacks at dawn and dusk are more likely.

The intent of Somali pirates is to hijack the ship and hold the crew for ransom. The usual practice is to keep the crew onboard as negotiations progress, keeping both the crew and the ship together. Seafarers have occasionally been separated by nationality and taken ashore. It is in the interests of the pirates to keep their captives alive, although cases of intimidation and torture have occurred.

Anti-ship missiles

Anti-ship missiles are long range, accurate and powerful weapons and have been used against military ships in the region. Their use against merchant ships associated with regional conflict cannot be discounted. Other ships may be hit if the missile controller targets the wrong ship or the missile homes in on an unintended target.

Sea mines

Sea mines have been used to deter and deny access to key ports in Yemen. These mines are usually tethered or anchored but may break free from moorings and drift into shipping lanes. Transiting merchant ships are not a target and it is recommended ships use the MSTC when passing through the area.

Water-Borne Improvised Explosive Devices

WBIED attacks have been used against warships and merchant ships in the southern Red Sea/BAM/western area of the Gulf of Aden.

Incidents have highlighted attacks by different groups operating in the region:

- WBIED used in the regional conflict have been aimed at harming those associated with the conflict. These boats have been unmanned and operated remotely.
- WBIED used by extremists have been aimed at merchant ships. These boats have been manned.

An attack involving a WBIED is likely to involve one or more speed boats operated by a number of individuals approaching and firing both small arms and RPGs. Masters should recognise the intent of these attacks is to cause damage and not necessarily to board the ship. Mitigation measures to prevent the speed boat making contact with the ship's hull are limited.

Section 3

Threat and risk assessment

Threat assessment

The threat assessment must include all regional security threats.

As part of every ship risk assessment prior to transit through the HRA the latest military threat advice must be obtained from UKMTO **www.ukmto.org** and threat assessments from MSCHOA **www.mschoa.org** (see annex A).

A **threat** is formed of capability, intent and opportunity.

Capability means 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 annex A.

If one side of the triangle is removed, then risk is minimised. The company/Master cannot influence either capability or intent, therefore BMP measures focus on minimising the opportunity.

Risk assessment

Risk assessment is an integral part of voyage planning within a safety management system. The risk assessment should identify measures for prevention, mitigation and recovery, which will mean combining statutory regulations with supplementary measures. Companies should also take account of these measures for ships transiting the VRA even if they do not enter the HRA.

Further guidance on risk assessments can be found in the *Global Counter Piracy Guidance* at **www.maritimeglobalsecurity.org**.

The risk assessment must consider but may not be limited to:

- Requirements of the Flag State, company, charterers and insurers.
- The threat assessment and geographical areas of increased risk.
- Background factors shaping the situation, e.g. traffic patterns and local patterns of life, including fishing vessel activity.
- Cooperation with military. An understanding of presence should be obtained from UKMTO.
- The embarkation of Privately Contracted Armed Security Personnel (PCASP).
- The ship's characteristics, vulnerabilities and inherent capabilities, including citadel and/or safe muster points 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.).

All voyages in this region require thorough advanced planning using all available information. The maritime threats are dynamic, and it is therefore essential that a detailed threat and risk assessment is completed for each voyage and activity within the region.

Section 4

Planning

Company planning

Together with the following, the output of the risk assessment will help develop the ship's voyage plan:

- Regular review of the threat and risk assessments. Plans should be updated as necessary.
- Review of the Ship Security Assessment (SSA), Ship Security Plan (SSP) and Vessel Hardening Plan (VHP).
- Guidance to the Master about the recommended route, updated plans and requirements for group transits and national convoys.
- Company mandated Ship Protection Measures (SPM).
- Due diligence of Private Maritime Security Companies (PMSCs) for the possible use of PCASP.
- Companies should consider the placement of hidden position transmitting devices as one of the first actions of hijackers is to disable all visible communication and tracking devices and aerials.
- Review of company manning requirements. Consider disembarking of non-essential crew.
- Crew training plans.

Information security

To avoid critical voyage information falling into the wrong hands the following is advised:

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

Ship Master's Planning

Security is a key part of any voyage plan.

Prior to entering the Voluntary Reporting Area

- Obtain the latest threat information.
- Check the latest NAVAREA warnings and alerts.
- Implement VRA/MSCHOA vessel registration and reporting requirements as highlighted in section 6 and annexes D and E.
- If used, confirm PCASP embarkation plan.
- Confirm propulsion can operate at full speed.

Prior to entering the High Risk Area

- Implement security measures in accordance with the SSP.

Brief crew and conduct drills

The crew should be fully briefed on the preparations and drills should be conducted with the SPM in place. The plan should be reviewed and all crew briefed on their duties, including familiarity with the alarm that signals an attack, an all-clear situation and the appropriate response to each. The drills should test:

- The SPM, including testing the security of all access points.
- Lock down conditions, including crew safety considerations.
- The bridge team's security knowledge.
- The crew's understanding of any different actions required in the event of a pirate attack compared to other types of attack.

Other considerations

- Prepare and test an emergency communication plan. Masters are advised to prepare an emergency communication plan, to include all essential emergency contact numbers (see annex A) and prepared messages, which should be at hand or permanently displayed near all external communications stations including safe muster point and/or the citadel. Communication devices and the Ship Security Alert System (SSAS) should be tested.
- Define the ship's Automatic Identification System (AIS) policy. It is recommended that AIS should remain switched on throughout passages through passages through the VRA and HRA, to ensure militaries can track the ship, but restrict data to ship's identity, position, course, speed, navigational status and safety related information.
- Reschedule planned maintenance on voyage critical equipment for transit of an HRA.

On entering the High Risk Area

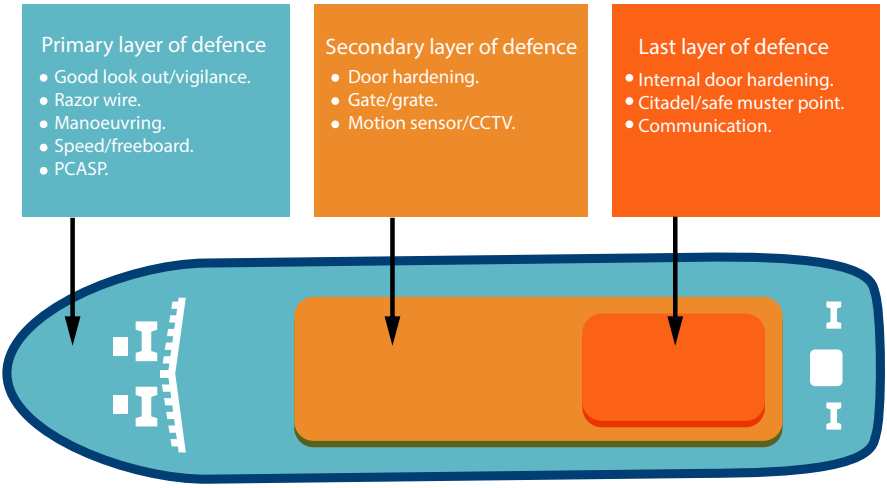
- Submit ship reports as highlighted in section 6 and annexes D and E.
- Monitor latest threat information.
- Ensure all access points are limited and controlled.
- Avoid drifting, waiting, anchoring and slow steaming, particularly in the MSTC.
- Minimise use of VHF and use email or a secure satellite telephone instead. Where possible only answer known or legitimate callers on the VHF, bearing in mind that imposters are possible.

Section 5

Ship Protection Measures

This section highlights proven SPM that provide layered protection. The BMP is based on regional experience of attacks and will continue to evolve as methods change.

The implementation of SPM will be identified during the voyage planning process. Companies may wish to consider making further alterations to the ship beyond the scope of this BMP, and/or providing additional equipment and/or personnel as a means of further reducing the risk of attack.



Watch keeping and enhanced vigilance

The Master should implement the following actions to assist in raising vigilance on board.

- Provide additional, fully-briefed lookouts.
- Maintain an all-round lookout from an elevated position.
- Consider shorter rotation of the watch period to maximise alertness of the lookouts.
- Maintain sufficient binoculars for the enhanced bridge team, preferably anti-glare.
- Consider the use of thermal imagery optics and night vision aids as they provide a reliable all-weather, day and night surveillance capability.
- Maintain a careful radar watch and monitor all navigational warnings and communications, particularly VHF and GMDSS alerts.
- Consider placing well-constructed dummies at strategic locations around the ship to give the impression of greater numbers of crew on watch.

- Consider using CCTV and fixed search lights for better monitoring. Fixed search lights can deter approaches from the stern.
- Mount anti-piracy mirrors on the bridge wings to make looking aft easier.

An effective lookout is the most effective method of ship protection. It can help identify a suspicious approach or attack early on, which allows defences to be deployed.

Manoeuvring

The Master and officers should practice manoeuvring the ship to ensure familiarity with the ship's handling characteristics. The Master should also practice avoidance manoeuvres while maintaining the best possible speed. Experience has shown that such action can defeat even a lengthy and determined attack as creation of hydrostatic pressure can have a better defensive impact than speed.

Avoidance manoeuvres should only be practiced when it is safe to do so.

Alarms

The ship's alarms inform the ship's crew that an attack is underway and warn the attacker that the ship is aware and is reacting. In addition, continuous sounding of the ship's whistle may distract the attackers.

It is important that:

- The alarms are distinctive to avoid confusion.
- 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 over the accommodation and deck PA system, where fitted.
- Drills are carried out to ensure that the alarm is heard throughout the ship. The drill will confirm the time necessary for all crew to move to a position of safety.

Physical barriers

Physical barriers are intended to make it as difficult as possible for attackers to gain access to ships by increasing the difficulty of the climb for those trying to illegally board. When planning the placement of barriers special consideration should be given to ships with sunken poop decks.

Razor wire

Also known as barbed tape. It creates an effective barrier if properly rigged and secured. The quality of razor wire varies considerably and lower quality razor wire is less effective. The following is recommended:

- Use a high tensile concertina razor wire with coil diameters of 730mm or 980mm. This is difficult to cut with hand tools.
- Use a double roll. If this is not possible, place a single high-quality roll outboard of the ship's structure.
- Secure razor wire to the ship properly, to prevent attackers pulling the wire off. For example, attach at least every third wire ring to ship's railings and rig a steel cable through its core.
- Use personal protective equipment and wire hooks to move and install razor wire.
- Obtain razor wire in short sections, e.g. 10m, so that it is easier and safer to move.
- Keep razor wire clear of mooring fairleads when at terminals so that it does not interfere with mooring operations.

Other physical barriers

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

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 unauthorised boat to remain alongside and makes it significantly more difficult to climb aboard.
- It is recommended hoses and foam monitors (delivering water) are fixed in position to cover likely access routes and are remotely operated. Manual activation is not recommended as this may place the operator in an exposed position.
- Improved water coverage may be achieved by using fire hoses in jet mode and using 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 with spray nozzles produce a water curtain covering larger areas.
- Foam can be used, but it must be in addition to a ship's standard fire fighting equipment stock. Foam is disorientating and very slippery.
- The use of all available fire and general service pumps may be required to ensure all defences operate efficiently.
- Additional power may be required when using 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.

Enhanced bridge protection

The bridge is usually the focal point of an attack. In some situations, attackers direct their weapon fire at the bridge to intimidate the ship's crew to slow or stop the ship. If pirates board the ship, they usually make for the bridge to enable them to take control.

The following enhancements may be considered:

- 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 an RPG.
- Sandbags can provide additional protection on the bridge wings. They should be regularly checked to ensure that they have not degraded.

Control of access to accommodation and machinery spaces

It is important to control access routes to the accommodation and machinery spaces to deter or delay entry. Effort must be directed at denying access to these spaces.

- Escape routes must remain accessible to seafarers in the event of an emergency.
- Where the door or hatch is located on an escape route from a manned compartment, it is essential it can be opened from the inside. Where the door or hatch is locked it is essential a means of opening the door from the inside is available.

- Doors and hatches providing access to the bridge, accommodation and machinery spaces should be properly secured to prevent them being opened from the outside.
- 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.
- Block external stairs or remove ladders on the accommodation block to prevent use and to restrict external access to the bridge.
- Doors and hatches that must be closed for watertight integrity should be fully dogged down in addition to any locks. Where possible, additional securing mechanisms, such as wire strops, may be used.
- 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.
- Pirates have been known to gain access through portholes and windows. The fitting of steel bars to portholes and windows will prevent this.
- Procedures for controlling access to accommodation, machinery spaces and store rooms should be briefed to the crew.
- The attackers must be denied access to ship propulsion.

Safe muster points and/or citadels

The company risk assessment and planning process should identify the location of a safe muster point and/or a citadel within a ship.

Safe muster points

A safe muster point is a designated area chosen to provide maximum physical protection to the crew and will be identified during the planning process.

If the threat assessment identifies risks that may result in a breach of hull on or below the waterline then a safe muster point above the waterline must be identified. In many ships, the central stairway may provide a safe location as it is protected by the accommodation block and is above the waterline.

To minimise the effect of an explosion, consideration should be given to the likely path of the blast. The safe muster point should be selected with this in mind.

Citadels

A citadel is a designated area where, in the event of imminent boarding, all crew may seek protection. A citadel is designed and constructed to resist forced entry. The use of a citadel cannot guarantee a military or law enforcement response.

Well-constructed citadels with reliable communications (ideally satellite phone and VHF) must be supplied with food, water and sanitation. Control of propulsion and steering can offer effective protection during an attack. If citadels are used, they must complement, not replace, all other SPM.

The use of the citadel must be drilled and the SSP should define the conditions and supporting logistics for its use.

It is important to note that military forces are likely to apply the following criteria before boarding a ship:

- All the crew must be accounted for and confirmed in the citadel.
- Two-way communication with the citadel.

The Master should decide when to use the citadel.

Other measures

Closed circuit television

Once an attack is underway it may be difficult to assess whether the attackers have gained access to the ship. The use of CCTV coverage allows a degree of monitoring of the progress of the attack from a less exposed position. Some companies can monitor and record the CCTV from ashore, which will be of value when provided to the military. The following should be considered:

- CCTV cameras for coverage of vulnerable areas, particularly the poop deck and bridge.
- CCTV monitors located on the bridge and at the safe muster point/citadel.
- CCTV footage may provide useful evidence after an attack and should be retained.

Lighting

Lighting is important and the following is recommended:

- Weather deck lighting around the accommodation block and rear facing lighting on the poop deck to demonstrate awareness.
- If fitted, search lights ready for immediate use.
- Once attackers have been identified or an attack commences, over side lighting, if fitted, should be switched on. This will dazzle the attackers and help the ship's crew to see them.
- At night, only navigation lights should be exhibited.
- Navigation lights should not be switched off at night as this a contravention of international regulations and the risk of collision is higher than that of being attacked.
- At anchor, deck lights should be left on as well-lit ships are less vulnerable to attack.
- The ability to turn off all internal accommodation lights to deter pirates from entering or disorientate those who may already have entered.

Deny the use of ship's tools and equipment

It is important to secure ship's tools or equipment that may be used to gain entry to the ship. Tools and equipment that may be of use to attackers should be stored in a secure location.

Protection of equipment stored on the upper deck

- Consideration should be given to providing ballistic protection to protect gas cylinders or containers of flammable liquids.
- Excess gas cylinders should be stored in a secure location or, if possible, landed prior to transit.

Private Maritime Security Companies

This section provides guidance on the employment of PMSCs. PMSCs may offer armed or unarmed services. Further guidance on the use of armed services (PCASP) is given below.

BMP does not recommend or endorse the general use of PMSCs onboard merchant ships; this is a decision taken by individual ship operators where permitted by the ship's Flag State and any littoral states. However, the use of experienced and competent unarmed PMSCs 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.

Any decision to engage the services of a PMSC should consider:

- The current threat and risk environment.
- The output of the company risk assessment.
- Voyage plan requirements.
- Ship speed.
- Freeboard.
- Type of operations, e.g. seismic survey or cable laying.
- Levels of protection provided by navies, coastguards and maritime police.

Some Flag States do not allow the deployment of PMSC.

It is recommended that shipping companies only employ PMSCs who are accredited to the current ISO 28007-1:2015 *Guidelines for Private Maritime Security Companies (PMSC) providing privately contracted armed security personnel (PCASP) on board ships*.

A PMSC contract must:

- Be between the technical manager and the PMSC.
- Not prejudice the ship's insurance cover arrangements.
- Ensure the PMSC has insurance policies that are current and compliant with the requirements of the contract.
- Clearly identify the procedure for the use of force.
- Confirm the Master's overriding authority.

Privately Contracted Armed Security Personnel

Any decision to engage the services of PCASP should consider the guidance above for PMSC as well as the following.

BMP does not recommend or endorse the general use of PCASP onboard merchant ships; this is a decision taken by individual ship operators where permitted by the ship's Flag State and any littoral states.

Companies must check the credentials and licenses/permits of the PMSC, and where appropriate the PCASP, to ensure they have been issued by an appropriate authority and are operating legally against identified threats.

Some Flag States do not allow the deployment of PCASP. Some Flag States provide military Vessel Protection Detachments (VPDs) instead of PCASP. A VPD may be provided by another State, subject to Flag State approval. In some cases, the deployment of either PCASP or VPDs must be reported and acknowledged by the Flag State and reported when entering the VRA (see section 6 and annexes D and E).

Master's overriding authority

If private security contractors are embarked, there must be a clear understanding of the overriding authority of the Master.

The Rules for the Use of Force (RUF) under which the PCASP operate must be acceptable to the Flag State and the company.

The Master and PCASP should:

- Clearly understand and acknowledge the RUF as outlined in the contract.
- Have documentation authorising the carriage of weapons and ammunition.
- Ensure all incidents involving the use of weapons and armed force are reported at the earliest instance to the Flag State and the Chief Security Officer (CSO).

The PCASP must:

- Act in accordance with the agreed RUF, which should provide for a graduated, reasonable, proportionate and demonstrably necessary escalation in the application of force in defence of crew on the ship.

PCASP should only be used as an additional layer of mitigation and protections and not as an alternative to other measures. The decision to carry PCASP is an output of the company risk assessment and a ship that traverses the HRA without PCASP on board can be considered in full compliance with the BMP. The ship's crew must not handle or use firearms.

Section 6

Reporting

All ships are strongly encouraged to inform military organisations of their movement as this is essential to improve military situational awareness and their ability to respond. Once ships have commenced their passage it is important this reporting continues and the guidelines in this section and annexes C, D and E are adopted to ensure common understanding. The two principal military organisations to contact are the UK Maritime Trade Operations (UKMTO) and Maritime Security Centre – Horn of Africa (MSCHOA).

UKMTO

UKMTO acts as the primary point of contact for merchant ships and their CSOs, providing liaison with military forces in the region. UKMTO administers the Voluntary Reporting Scheme, under which merchant ships are encouraged to send regular reports. These include:

1. Initial report (upon entering the VRA).
2. Daily reports (update on ship's position, course and speed).
3. Final reports (upon departure from VRA or arrival in port).
4. Reports of suspicious/irregular activity (when necessary).

UKMTO is able to communicate with ships and CSOs directly, in order to disseminate Warnings and Advisories of incidents within the region:

- Warnings: Simple messages describing that an incident has occurred in a Lat/Long and with a time. This is normally accompanied by direct UKMTO-to-ship telephone calls to all ships within a nominated radius of the incident to give ships the earliest possible alert.
- Advisories: This is the next tier of alerts to ships, normally of sightings/reports that are relevant within the region.

UKMTO offers regular information to ships on its website **www.ukmto.org** and in a weekly report summarising the previous week's activity. UKMTO is also able to offer Masters and CSOs the opportunity to conduct drills and exercises to support their passage planning in the region. Companies that are interested can contact UKMTO +44(0)2392 222060 or watchkeepers@ukmto.org.

Ships and their operators should complete both UKMTO vessel position reporting forms and register with MSCHOA.

MSCHOA

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

When departing the VRA, ships should be aware of adjacent regional reporting requirements, e.g.: NATO Shipping Centre (Mediterranean – Chart Q6010) and ReCAAP Information Sharing Center/Singapore Information Fusion Center (SE Asia – Chart Q6012).

EU NAVFOR and the Combined Maritime Forces (CMF) produce Industry Releasable Threat Assessments (IRTAs) to aid risk management for companies. The threat assessments use military knowledge and intelligence to present a common understanding of the threats and trends in the region. The IRTAs are complimented by Industry Releasable Threat Bulletins (IRTBs), which cover specific events. These documents are an important resource and should be considered as part of the threat and risk assessment process.

The role of the seafarer in improving maritime safety and security in the region

Although some of the maritime threats and crimes committed do not directly endanger seafarers there is the opportunity for them to contribute to maritime security.

Experience has shown that maritime security cannot be improved by the actions of law enforcement agencies and militaries alone; seafarers operating in the region can help. This is more important in the seas off the coast of Somalia and Yemen where navies, coastguards and law enforcement agencies have limited resources.

Masters are encouraged to report suspicious activity and provide as much detail as possible. If it is possible to do so without compromising safety, photographs, video and radar plot data of suspicious activity are of enormous value to the responsible authorities. If there is any doubt as to whether the activity is suspicious, ships are encouraged to report.

Reporting suspicious activity to UKMTO

UKMTO can advise on the types of activity of interest to the regional maritime community. A guide to help identify suspicious activity is in annex C and the suspicious/irregular activity report is in annex D. Often, seafarers do not report suspicious activity as they may be concerned observations could lead to further investigations by Port States and possible delay to the ship. UKMTO will forward information received in an anonymised form to the most appropriate agency empowered to act. While suspicious activity may appear inconsequential, when added to other reports it may be extremely valuable.

Section 7

Ships under attack

General

A ship may come under attack with little or no warning. Effective lookouts, both visual and radar, will help to ensure early detection.

Piracy attack

Pirates carrying weapons do not usually open fire until they are very close to the ship, e.g. within two cables.

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

In the event of a suspicious approach, or if in any doubt, call UKMTO without delay.

Approach stage

Effective lookouts may aid in identifying the nature of the attack, the threat profile of a piracy or other attack may initially look similar and it will not be until the attackers are close that the nature of the attack becomes apparent. In all cases, the following steps should be taken:

- If not already at full speed, increase to maximum to open the distance.
- Steer a straight course to maintain a maximum speed.
- Initiate the ship's emergency procedures.
- Activate the emergency communication plan.
- Sound the emergency alarm and make an attack announcement, in accordance with the ship's emergency communication plan.
- Make a mayday call on VHF Ch. 16. Send a distress message via the Digital Selective Calling (DSC) system and Inmarsat-C, as applicable.
- Activate the SSAS.
- Report the attack immediately to UKMTO (+44 2392 222060) by telephone.
- Ensure the AIS is switched on.

- Activate water spray.
- Ensure that all external doors and, where possible, internal public rooms and cabins are fully secured.
- All crew not required on the bridge or in the engine room should muster at the safe muster point or citadel as instructed by the Master.
- When sea conditions allow, consider altering course to increase an approaching skiff's exposure to wind/ waves.
- Sound the ship's whistle/foghorn continuously to demonstrate to any potential attacker that the ship is aware of the attack and is reacting to it.
- Check Vessel Data Recorder (VDR) is recording.
- PCASP, if present, will take agreed actions to warn off attackers.

Attack stage

As the attackers get close the following steps should be taken:

- Reconfirm all ship's crew are in the safe muster point or citadel as instructed by the Master.
- Ensure the SSAS has been activated.
- If not actioned, report the attack immediately to **UKMTO (+44 2392 222060)** by telephone.
- As the attackers close in on the ship, Masters should commence small alterations of helm whilst maintaining speed to deter skiffs from lying alongside the ship in preparation for a boarding attempt. These manoeuvres will create additional wash to impede the operation of the skiffs.
- Large amounts of helm are not recommended, as these are likely to significantly reduce a ship's speed.
- Check VDR data is being saved.
- PCASP, if present, will conduct themselves as governed by the RUF.

Actions on illegal boarding

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

- Take all way off the ship and then stop the engines.
- All remaining crew members to proceed to the citadel or safe muster point locking all internal doors on route.
- PCASP, if present, will follow procedures agreed with company and Master.
- Ensure all crew are present in the citadel or safe muster point. This includes the Master, bridge team and PCASP.

- Establish communications from the citadel with UKMTO and your company and confirm all crew are accounted for and in the citadel or safe muster point.
- Stay in the citadel until conditions force you to leave or advised by the military.
- If any member of the crew is captured it should be considered that the pirates have full control of the ship.

If control of the ship is lost

- All movement should be calm, slow and very deliberate. Crew members should keep their hands visible always and comply fully. This will greatly reduce the risk of violence.

Experience has shown that the pirates will be aggressive, highly agitated and possibly under the influence of drugs or alcohol.

DO be patient.

DO keep mentally active/occupied.

DO keep track of time.

DO reduce stress where possible by remaining physically active.

DO remain calm and retain dignity.

DO be positive (remember, authorities are working tirelessly to release you).

DO remember to leave any CCTV or audio recording devices running.

DO exactly what the attackers ask and comply with their instruction.

DO NOT take photographs.

DO NOT attempt to engage attackers.

DO NOT make movements which could be misinterpreted as being aggressive.

DO NOT be confrontational.

DO NOT resist.

Hijack – hostage situation

The model of pirate action off Somalia is to hijack the ship and hold the crew for ransom. It should be remembered it is in the interests of the pirates to keep the ship and crew safe.

Each company or organisation should have a policy in place to cover the eventualities of kidnap and ransom. The following principles serve as guidelines to surviving a kidnapping.

DO remain calm and maintain self-control.

DO be humble and respectful to the pirates.

DO look out for your colleagues' well-being.

DO stay together as a team, where possible.

DO accept the new pirate leadership.

DO maintain the hierarchy of rank.

DO try to establish normal communication with the pirates.

DO maintain personal hygiene.

DO save water and essentials.

DO be positive – many people are working to release you.

DO be patient and maintain routines (including your spiritual needs, as permitted by pirates).

DO try to keep your breathing regular.

DO meditate and keep mentally active.

DO respect religion: yours, your colleagues' and the pirates'.

DO NOT offer resistance.

DO NOT argue with pirates or your colleagues.

DO NOT take photographs.

DO NOT hide valuables.

DO NOT react emotionally.

DO NOT take drugs or alcohol.

DO NOT bargain with pirates for personal privileges.

In the event of military intervention

Brief and prepare the ship's crew to cooperate fully during any military action onboard and instruct crew as follows.

DO keep low to the deck and cover head with both hands.

DO keep hands visible.

DO be prepared to be challenged on your identity.

DO cooperate fully with military forces.

DO NOT make movements that could be interpreted as aggressive.

DO NOT take photographs.

DO NOT get involved in activity with military forces unless specifically instructed to.

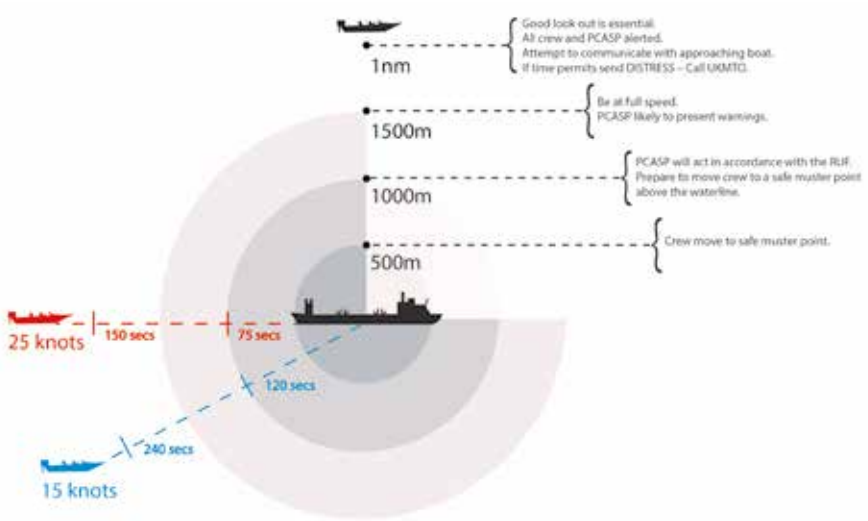
Attack from other threats

- **Anti-ship missiles** In the event or warning of a missile attack military advice should be followed. If no warning is received there will be no time to take any mitigations beyond a PA warning to the crew if a missile is spotted. It is unlikely merchant ships will be the intended target; Masters should be aware of the ship plot in their immediate vicinity and, if sea room allows, keep clear of naval and associated ships.
- **Sea mines** Ships should avoid all published or identified mine danger areas and maintain close liaison with military authorities. If operating close to mine danger areas, Masters should be aware tethered mines may break free and drift into shipping lanes. Ships should manoeuvre clear of floating objects and the forward area of the ship should be kept clear of crew. Effective lookouts are essential. Specific advice on self protective measures when operating in mine danger areas can be obtained from UKMTO.
- **WBIED attack** In the early stages of the attack it may not be possible to differentiate between a piracy or WBIED attack. Initial actions as highlighted in this guidance for the approach stage of a piracy attack should be followed. Military threat assessments may indicate areas where one type of attack is more likely than another. A speed boat with multiple people onboard is unlikely to be a WBIED as these are usually unmanned or have a solitary occupant.

  WBIED attacks may result in a breach of the ship's hull. The use of the safe muster point is recommended before entering a citadel located below the waterline.

Courtesy of the US Naval Institute

If a WBIED is anticipated, the time to react is very short. The figure below gives an example of possible reaction times.



The threat and risk assessment will identify areas where these threats occur which, if successful, may result in an explosion (commonly referred to as a blast). The Master should communicate to the crew prior to entering a threat area what position to take if a blast threat is detected. The Master may consider telling the crew to:

- Lie flat on the deck, as this may minimise exposure and may reduce the impact on the body from the blast.
- Adopt a brace position (arms/legs bent, hands holding onto something solid and feet firmly planted on the deck) to protect personnel from shock waves.
- Move away from a particular area, such as the port side, starboard side, poop deck or engine room.

Post a WBIED attack

- Ensure all crew and PCASP are accounted for.
- Send distress signal.
- Survey area where the blast occurred.
- Implement damage control.
- Call CSO and UKMTO.

Post incident actions and reporting

The period following an attack will be difficult as companies, Master and crew recover from the ordeal. It is important that seafarers receive timely and proper medical assessments, both physical and mental, and care following an attack or hostage situation. Companies should have emergency management plans in place to manage the effects from an attack from any of the identified threats on one of their ships. These plans should include the management of a long, drawn-out hostage negotiation situation, including support for the families of the kidnapped crew.

To give the investigating authorities the best chance of apprehending the perpetrators, it is important that evidence is preserved in the correct manner. Companies, Masters and crew should refer to IMO *Guidelines on Preservation and Collection of Evidence* A28/ Res. 1091 and other industry guidance.

Following any attack or suspicious activity, and after initial reporting of the event, it is vital that a detailed report is completed. A copy of the report should be sent to the company, the Flag State and appropriate authorities. It is important that any report is detailed and comprehensive. This will assist with full analysis and trends in threat activity.

Without supporting evidence, including witness statements from those affected by the incident, suspects are unlikely to be prosecuted.

Protection of evidence

The collection and protection of evidence is critical.

The Master and crew can protect a crime scene until the nominated law enforcement agency arrives by following these basic principles:

- Preserve the crime scene and all evidence if possible.
- 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, including hosing it down. Do not throw anything away, no matter how unimportant it may seem.
- Take initial statements from the crew.
- Take photographs of the crime scene from multiple viewpoints.
- Protect VDR for future evidence.
- Make a list of items taken (e.g. mobile phones with numbers).
- Facilitate access to the crime scene and relevant documentation for law enforcement authorities.
- Make crew available for interview by law enforcement authorities.

Investigation

Thorough investigation using all available evidence is critical.

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 incident the investigating authority will be determined by external factors including:

- Flag State.
- Ownership.
- Crew nationality.

Seafarers should always be treated with respect and as victims of crime.

The lead law enforcement agency will talk to the Master and crew to understand the sequence and circumstances of the event.

In a post hostage situation, law enforcement authorities may ask to conduct post-release crew debriefs and to collect evidence for investigations and prosecutions following captivity.

Advice

INTERPOL has a secure website to provide support to ship operators who have had their ships hijacked. INTERPOL's Maritime Task Force can assist in taking the appropriate steps to preserve the integrity of the evidence left behind at the crime scene. INTERPOL has a Command and Co-ordination Centre (CCC) that supports any of the 188-member countries faced with a crisis or requiring urgent operational assistance. The CCC operates in all four of INTERPOL's official languages (English, French, Spanish and Arabic) and is staffed 24 hours a day, 365 days a year. It is recommended that ship operators contact INTERPOL within three days of a hijacking of their ship.

INTERPOL may also be consulted to discuss the recommended practices for the preservation of evidence that could be useful to law enforcement agents pursuing an investigation. Contact details are: email os-ccc@interpol.int; telephone +33 472 44 7676.

Seafarer welfare

Seafarers and their families often have difficulty in expressing the need for assistance or even recognising that they need assistance following exposure to a security threat. The company should monitor the health, both physical and mental, of those exposed to piracy and other maritime security threats and if necessary provide independent support and other assistance, as may be appropriate. There is a range of humanitarian programmes aimed at assisting seafarers and their families effected by piracy or maritime crime, including the International Seafarers Welfare and Assistance Network and The Mission to Seafarers. See **www.seafarerswelfare.org** and **www.missiontoseafarers.org**.

ANNEX 2

Annex A

Contact details

Emergency contacts

United Kingdom Maritime Trade Operations

Email	watchkeepers@ukmto.org
Telephone (24hrs)	+44 2392 222060
Website	www.ukmto.org

Maritime Security Centre – Horn of Africa

Email	postmaster@mschoa.org
Telephone	+44 1923 958545 +44 1923 958700
Fax	+44 1923 958520
Website	www.mschoa.org

US Naval Cooperation and Guidance for Shipping

Email	cusnc.ncags_bw@me.navy.mil
Telephone (24hrs)	+973 3904 9583
Telephone (office)	+973 1785 1023

Useful contacts

International Maritime Bureau (IMB)

Email	piracy@icc-ccs.org
Telephone	+60 3 2031 0014
Fax	+60 3 2078 5769
Telex	MA34199 IMBPC1
Website	www.icc-ccs.org

INTERPOL

Email	os-ccc@interpol.int
Telephone (24hrs)	+33 472 44 76 76
Website	www.interpol.int

Adjacent regional reporting centres

Mediterranean

NATO Shipping Centre

Email	info@shipping.nato.int
Telephone (24hrs)	+44 1923 956574
Fax	+44 1923 956575
Website	www.shipping.nato.int

South East Asia

ReCAAP Information Sharing Centre

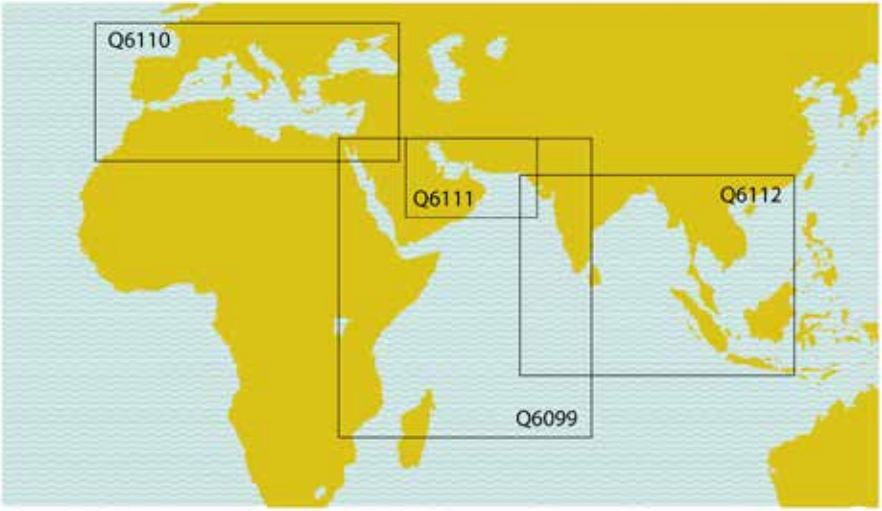
Email	info@recaap.org
Telephone	+65 6376 3063
Fax No	+65 6376 3066

Singapore Information Fusion Centre

Email	ifc_do@defence.gov.sg
Telephone	+65 9626 8965 (24/7) +65 6594 5728
Fax No	+65 6594 5734

Annex B

Maritime security charts



Maritime security charts contain safety-critical information to assist bridge crews in the planning of safe passages through high risk areas. All information has been gathered by the UKHO through work with NATO and other government organisations, ensuring each chart has the most accurate, up-to-date and verified information available.

Each maritime security chart includes:

- Information about dangers to the security of navigation including piracy, terrorism, embargoes, mine warfare, exclusion zones, blockades and illegal fishing. This information, when used alongside official navigational charts, can help to ensure the safety of ships, crew and cargo.
- General security advice, self-protective measures, security procedures and regional contacts, as well as routeing and reporting requirements implemented by military or security forces.

Annex C

Common understanding

It is important to have a common understanding when reporting attacks and suspicious activity.

The following are guidelines to assist in assessing what is an attack or what constitutes suspicious activity.

Attacks

- The use of violence against the ship, its crew or cargo, or any attempt to use violence.
- Unauthorised attempts to board the ship where the Master suspects the persons are pirates or other unauthorised persons.
- If weapons or RPGs are fired.
- Attempts to place a WBIED against the hull.
- Sighting of missile firing.
- An actual boarding, whether successful in gaining control of the ship or not.
- Attempts to overcome the SPM using:
    - Ladders.
    - Grappling hooks.
    - Weapons deliberately used against or at the ship.

Suspicious activity

- The number of crew onboard relative to its size.
- The Closest Point of Approach.
- The existence of unusual and non-fishing equipment onboard, e.g. ladders, climbing hooks or large amounts of fuel.
- One vessel towing multiple skiffs or has skiffs onboard.
- The type of vessel is unusual for the current location.
- Small boats operating at high speed.
- If a vessel appears unmanned.
- The vessel is not transmitting on AIS.
- The vessel is not flying a Flag.
- Vessel is flying two or more flags simultaneously.
- Skiffs operating far from the coast.
- Vessels fishing outside of normal fishing zones.
- Windows of vessel covered or blanked out.

- Dhows/skiffs rafted up.
- No lights during hours of darkness.
- Skiffs with two or more outboard motors.
- Dhows/skiffs stopped in the water, no evidence of fishing.
- Vessels loitering East of Socotra, South of the Makran Coast or in the vicinity of Zanzibar, Dar es Salaam, Pemba, Salalah, Ras Fartek or the IRTC.
- Packages hanging outboard of a vessel.
- Excessive communications antennas.

This is not an exhaustive list. Other events, activity and vessels may be deemed suspicious by the Master of a merchant ship having due regard to their own seagoing experiences within the region and information shared amongst the maritime community.

If in doubt, report and contact UKMTO.

Annex D

UKMTO reporting forms

UKMTO vessel position reporting forms

Once a ship has transmitted an initial report on entering the VRA, UKMTO will request daily reports be transmitted. Upon reaching port or upon exiting the VRA, UKMTO will request a final report. The following forms are provided below and are available at **www.ukmto.org**:

- Initial report.
- Daily report.
- Final report.
- Suspicious/irregular activity report.

UKMTO vessel position reporting form - initial report

1	Ship Name
2	Flag
3	IMO Number
4	INMARSAT Telephone Number
5	Time and Position
6	Course
7	Passage Speed
8	Freeboard
9	Cargo
10	Destination and Estimated Time of Arrival
11	Name and contact details of Company Security Officer
12	Nationality of Master and Crew
13	Armed/unarmed security team embarked

ANNEX 2

UKMTO vessel position reporting form – daily/transit position report

1	Ship Name
2	Ship's Call Sign and IMO Number
3	Time of Report in UTC
4	Ship's Position
5	Ship's Course and Speed
6	Any other important information*
7	ETA point A/B IRTC (if applicable)

**Other important information could be change of destination or ETA, number of UK crew on board, etc.*

UKMTO vessel position reporting form - final report

1	Ship's name
2	Ship's Call Sign and IMO Number
3	Time of Report in UTC
4	Port or position when leaving the voluntary reporting area

UKMTO suspicious/irregular activity report

1	Ship's name
2	Ship's Call Sign and IMO Number
3	Time of Report in UTC
4	Ship's Position
5	Ship's Course and Speed
6	Sighting of suspicious activity. Time, position, brief description of craft and activity witnessed

Note: Where possible include any imagery to aid military appreciation.

Follow-up report to UKMTO and MSCHOA

Following any attack or suspicious activity, it is vital that a detailed report of the event is provided to UKMTO and MSCHOA. It is helpful to provide a copy of the report to the IMB.

Annex E

Maritime Security Centre – Horn of Africa reporting forms

MSCHOA vessel registration and incident reporting

Registration with MSCHOA ensures a ship is monitored by military counter piracy forces during its transit of the HRA. In addition, regular threat assessment updates, warnings and the latest self-protection information are made available to shipping companies and Masters who register.

Registration is required within the MSCHOA Vessel Registration Area as highlighted on UKHO Chart Q6099.

The form to 'Register a Vessel's Movements' is available on the MSCHOA website and UKHO Chart Q6099. The following should be noted:

- There are two principal methods to register your ship's movement with MSCHOA.
  - **Online** at **www.mschoa.org** (note you will need to register with MSCHOA for access, this can be done following the register tab on the website).
  - **Offline.** A downloadable form is available from **www.mschoa.org** or it can be requested from **postmaster@mschoa.org**. This form was updated in March 2018 to make offline registration simpler for ships with sporadic internet connectivity to register.

If the above options are not possible a ship can be registered by sending an email with the subject heading **MSCHOA Vessel Registration** to postmaster@mschoa.org with the information in the table below. Items marked with an * are mandatory.

Vessel Details

Ship Name *	Flag State *
IMO Number *	MMSI Number *
Call Sign *	Ship's Master
Primary Email *	Secondary Email
Ship contact number *	Ship contact email *
Owner name	Operator name
Operator address	DPA name
DPA telephone	DPA email

ANNEX 2

Movement Details

Entry Point to MSCHOA vessel registration area * (78°E/10°S/23°N/Suez/Port)	Entry Date/Time to MSCHOA vessel registration area * (DD/MM/YYYY) (HH) (MM)
Exit Point from MSCHOA vessel registration area * (78°E/10°S/23°N/Suez/Port)	Exit Date/Time to MSCHOA vessel registration area * (DD/MM/YYYY) (HH) (MM)
Do you intend to transit the IRTC?	
ETA to IRTC (times are in UTC/ Zulu time) *	
Direction * (East/West)	
Do you intend to join a group transit?	Do you intend to join a National Convoy?
	Which National Convoy are you joining? *
Crew numbers and nationalities	Draught
Freeboard of lowest accessible deck in Metres(M) *	Planned Transit Speed *
Vessel's Maximum Speed *	Cargo (Crude Oil/Clean Oil/Arms/ Chemicals/ Gas/Passengers/Bulk Cargo/ Containers/Fishing/Ballast/ Others … Please Specify)
	Hazardous cargo
Next Port of Call	Last Port of Call
Number of Armed Security personnel on board?	Nationality of armed security team?

ANNEX 2

Follow-up report to MSCHOA and UKMTO

Following any attack or suspicious activity, it is vital that a detailed report of the event is provided to UKMTO and MSCHOA. It is also helpful to provide a copy of the report to the IMB.

Incident report; vessel particulars/details

It is recognised that during an incident time may be short and crew will be under a number of pressures and stresses. Those lines marked with an * are those that, in extremis, are the key requirements that must be reported. Without this data responses cannot be planned or mounted and assessments will be incomplete and may be inaccurate.

INCIDENT REPORTING PART ONE – VESSEL DETAILS				
Line			Responses / Inclusions	Format
(a)	(b)			(d)
IDENTITY	1.1	A*	SHIP NAME	PLAIN TEXT
		B*	IMO NUMBER	PLAIN TEXT
		C	FLAG	PLAIN TEXT
		D	CALL SIGN	PLAIN TEXT
		E	OWNER NAME & CONTACT DETAILS	PLAIN TEXT
		F	Company Security Officer / Designated Person Assure CONTACT DETAILS	PLAIN TEXT
CREW / CARGO	1.2	A	CREW NUMBER	PLAIN TEXT
		B	CREW NATIONALITIES	PLAIN TEXT
		C	CAPTAIN / MASTER NATIONALITY	PLAIN TEXT
		D	CARGO	PLAIN TEXT
		E	CARGO SIZE / QUANTITY	PLAIN TEXT
ROUTE / SCHEDULE	1.3	A	LAST PORT OF CALL (LPOC)	PLAIN TEXT
		B	LAST PORT OF CALL DATE	PLAIN TEXT
		C	NEXT PORT OF CALL (NPOC)	PLAIN TEXT
		D	NEXT PORT OF CALL DATE	PLAIN TEXT
		E	SEA DAYS SINCE LAST PORT	PLAIN TEXT

ANNEX 2

INCIDENT REPORTING PART TWO – INCIDENT DETAILS				
Line			Responses / Inclusions	Format
(a)	(b)			(d)
DETAILS	2.1*		TIME OF REPORT	DTG
	2.2	A*	INCIDENT LOCATION	LAT / LONG
		B*	SPEED AND HEADING AT TIME OF INCIDENT	PLAIN TEXT
	2.3	A*	INCIDENT START TIME	DTG
		B*	INCIDENT END TIME	DTG
		C	WEATHER CONDITIONS DURING EVENT	PLAIN TEXT
INCIDENT	2.4	A*	SIGHTING / APPROACH / COMMUNICATION / ATTACK / BOARDING	SELECT
		B	AREA(S) OF VESSEL TARGETED	PLAIN TEXT
SUSPECTS	2.5	A*	NUMBER OF SUSPECT CRAFT	NUMBER
		B	NUMBER OF SUSPECT INDIVIDUALS	NUMBER
		C	NOT KNOWN / CIVILIAN DRESS / UNIFORMS / MIX	SELECT
		D	ETHNICITY / LANGUAGES	PLAIN TEXT
WEAPONS	2.6	A*	NONE SEEN / SIGHTED / SHOTS FIRED	SELECT
		B	PISTOLS / RIFLES / MACHINE GUNS / GRENADE LAUNCHERS	SELECT
LADDERS	2.7	A	NONE SEEN / SUSPECTED / SIGHTED / USED	SELECT
		B	ADDITIONAL INFORMATION	PLAIN TEXT
CRAFT	2.8	A*	TYPE: WHALER / DHOW / FISHING VESSEL / MERCHANT VESSEL	SELECT
		B	DESCRIPTION OF VESSEL (COLOUR, NAME, FEATURES)	PLAIN TEXT

YOUR VESSEL	2.9	A*	CITADEL / SECURE AREA	YES / NO
		B*	NO SECURITY TEAM / UNARMED TEAM / ARMED TEAM	SELECT
		C	HEIGHT OF FREEBOARD AT THE TIME OF INCIDENT	PLAIN TEXT
		D	SELF PROTECTION MEASURES IN PLACE BEFORE INCIDENT	PLAIN TEXT
		E	DEFENCE MEASURES EMPLOYED	YES / NO
		F	OTHER	PLAIN TEXT
YOUR RESPONSE	2.10	A*	ALARM SOUNDED	YES / NO
		B*	CREW MUSTERED IN CITADEL	YES / NO
		C*	INCREASED SPEED / EVASIVE MANOEUVRES	SELECT
		D*	DESCRIPTION	SELECT
		E	PAST SHOWED WEAPONS / WARNING SHOTS / AIMED SHOTS / NO PAST	PLAIN TEXT
		F	WAS INCIDENT REPORTED TO AUTHORITIES? IF SO TO WHOM?	PLAIN TEXT
STATUS	2.11	A*	INCIDENT FINISHED / ONGOING	SELECT
		B	INCIDENT ENDED BY SUSPECTS / OWN VESSEL	YES / NO
		C	DETAIL	YES / NO

ANNEX 2

INCIDENT REPORTING PART THREE – STATUS AND SUPPORT REQUESTS				
Line			Responses / Inclusions	Format
(a)	(b)			(d)
STATUS	3.1	A*	VESSEL SAFE / UNSAFE / UNDER ATTACK / BOARDED	SELECT
		B	VESSEL UNDERWAY / VESSEL STATIC	SELECT
		C*	UNDER OWN POWER / SUPPORTED / WITHOUT POWER	SELECT
		D	NO DAMAGE / MINOR DAMAGE / MAJOR DAMAGE	SELECT
DAMAGE / MEDICAL	3.2	A*	DAMAGE DETAILS	PLAIN TEXT
		B	CREW AT STATIONS / CREW IN CITADEL / CREW OFF SHIP	SELECT
		C	CREW INJURIES	NUMBER
		D	INJURY DETAILS	PLAIN TEXT
		E	CREW FATALITIES	NUMBER
		F	FATALITY DETAILS	PLAIN TEXT
INTENTIONS	3.3	A*	CONTINUE AS PLANNED / RE-ROUTING	SELECT
		B*	REPAIR DAMAGE / ABANDON SHIP / SURRENDER CONTROL	PLAIN TEXT
		C	CURRENT SPEED	PLAIN TEXT
		D	CURRENT HEADING	PLAIN TEXT
		E	OTHER	PLAIN TEXT

ANNEX 2

IMAGERY	3.4	A	WAS THE INCIDENT RECORDED?	YES / NO
		B	CCTV FOOTAGE / PHOTOGRAPHS	SELECT
		C	IMAGERY ATTACHED (IF AVAILABLE PLEASE ATTACH)	YES / NO
ADDITIONAL INFORMATION	3.5	A	ANY OTHER INFORMATION WHICH MAY ASSIST?	PLAIN TEXT
		B	PLEASE ATTACH WITH THIS REPORT – A BRIEF DESCRIPTION / FULL REPORT / MASTER – CREW STATEMENT OF THE ATTACK	PLAIN TEXT

Annex F

Additional guidance for vessels engaged in fishing

This guidance for vessels engaged in fishing has been provided by the following national fishing industry associations:

- **OPAGAC** – Organizacion de Productores Asociados de Grandes Atuneros Congeladores.
- **ANABAC** – Asociacion Nacional de Armadores de Buques Atuneros Congeladores.

Recommendations to vessels in fishing zones

- Non-Somali fishing vessels should avoid operating or transiting within 200nm of the coast of Somalia, irrespective of whether they have been issued with licenses to do so.
- Do not start fishing operations when the radar indicates the presence of unidentified boats.
- If polyester skiffs of a type typically used by pirates are sighted, move away from them at full speed, sailing into the wind and sea to make their navigation more difficult.
- Avoid stopping at night. Be alert and maintain bridge, deck and engine-room watch.
- During fishing operations, when the vessel is more vulnerable, be alert and maintain radar watch to give maximum notice to your crew and the state authorities if an attack is in progress.
- While navigating at night, use only the mandatory navigation and safety lights to prevent the glow of lighting attracting pirates, who are sometimes in boats without radar and are waiting.
- If the vessel is drifting while fishing at night, keep guard at the bridge on deck and in the engine room. Use only mandatory navigation and safety lights.
- The engine must be ready for an immediate start-up.
- Keep away from unidentified ships.
- Use VHF as little as possible to avoid being heard by pirates and to make location more difficult.
- Activate the AIS when maritime patrol aircraft are operating in the area to facilitate identification and tracking.

Identification

- Managers are strongly recommended to register their fishing vessels with MSCHOA for the whole period of activity off the coast of Somalia. This should include communicating a full list of the crewmen on board and their vessels' intentions, if possible.
- Carry out training prior to passage or fishing operations in the area.
- Whenever fishing vessels are equipped with Vessel Monitoring System (VMS) devices, their manager should provide MSCHOA with access to VMS data.
- Fishing vessels should always identify themselves upon request from aircraft or ships from any international or national anti-piracy operation.
- Military, merchant and fishing vessels should respond without delay to any identification request made by a fishing vessel being approached (to facilitate early action to make escape possible, especially if the vessel is fishing).

In case of attack

- In case of an attack or sighting a suspicious craft, warn the authorities (UKMTO and MSCHOA) and the rest of the fleet.
- Communicate the contact details of the second Master of the vessel (who is on land) whose knowledge of the vessel could contribute to the success of a military intervention.
- Recommendations **only for Purse Seiners:**
    - Evacuate all crew from the deck and the crow's nest.
    - If pirates have taken control of the vessel and the purse seine is spread out, encourage the pirates to allow the nets to be recovered. If recovery of the purse seine is allowed, follow the instructions for its stowage and explain the functioning of the gear to avoid misunderstanding.

Annex G

Additional advice for leisure craft, including yachts

Leisure craft should make early contact in advance with the naval/military authorities to determine if the VRA area is safe to transit; regional activity has indicated attacks occur on both large and small vessels. Transit close to areas of conflict should be avoided. Close contact should be maintained with UKMTO throughout any voyage.

See the MSCHOA (**www.mschoa.org**) and the International Sailing Federation (**www.sailing.org**) for the most up-to-date information.

Annex H

Definitions and abbreviations

Definitions

The following definitions to term and categorise attacks and suspicious incidents that are reported from shipping inside the VRA may help. This ensures the consistent identification of patterns and trends.

Armed robbery The Code of Practice for the Investigation of the Crimes of Piracy and Armed Robbery against Ships, highlights armed robbery against ships consists of:

- Any illegal act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, committed for private ends and directed against a ship or against persons or property on board such a ship, within a State's internal waters, archipelagic waters and territorial sea.
- Any act of inciting or of intentionally facilitating an act described above.

Attack An attack, as opposed to an approach, is where a ship has been subjected to an aggressive approach by an unidentified craft AND weapons have been discharged.

Hijack A hijack is where attackers have illegally boarded and taken control of a ship against the crew's will. Hijackers will not always have the same objective (armed robbery, cargo theft or kidnapping).

Illegal boarding An illegal boarding is where attackers have boarded a ship but HAVE NOT taken control. Command remains with the Master. The most obvious example of this is the citadel scenario.

Piracy Piracy is defined in the 1982 United Nations Convention on the Law of the Sea (UNCLOS) (article 101). However, for the purposes of these BMP, it is important to provide clear, practical, working guidance to the industry to enable accurate and consistent assessment of suspicious activity and piracy attacks.

The following may assist in assessing what is a piracy attack. A piracy attack may include but is not limited to:

- The use of violence against the ship or its personnel, or any attempt to use violence.
- Attempt(s) to illegally board the ship where the Master suspects the persons are pirates.
- An actual boarding whether successful in gaining control of the ship or not.
- Attempts to overcome the SPM by the use of:
    - Ladders.
    - Grappling hooks.
    - Weapons deliberately used against or at the ship.

Suspicious or aggressive approach Action taken by another craft may be deemed suspicious if any of the following occur (the list is not exhaustive):

- A definite course alteration towards a ship associated with a rapid increase in speed by the suspected craft, which cannot be accounted for by the prevailing conditions.
- Small craft sailing on the same course and speed for an uncommon period and distance, not in keeping with normal fishing or other circumstances prevailing in the area.
- Sudden changes in course towards the ship and aggressive behaviour.

Abbreviations

AIS	Automatic Identification System
BAM	Bab el Mandeb
CMF	Combined Maritime Forces
CSO	Chief Security Officer
DSC	Digital Selective Calling
EU NAVFOR	European Union Naval Force
HRA	High Risk Area
IMB	International Maritime Bureau
IMO	International Maritime Organization
IRTA	Industry Releasable Threat Assessment
IRTB	Industry Releasable Threat Bulletin
IRTC	Internationally Recommended Transit Corridor
JWC	Joint War Committee
MSC	Maritime Safety Committee
MSCHOA	Maritime Security Centre – Horn of Africa
MSTC	Maritime Security Transit Corridor
NATO	North Atlantic Treaty Organisation
PAG	Pirate Action Group
PCASP	Privately Contracted Armed Security Personnel
PMSC	Private Maritime Security Company
RECAAP	Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia
RPG	Rocket Propelled Grenade

RUF	Rules for the Use of Force
SPM	Ship Protection Measures
SSA	Ship Security Assessment
SSAS	Ship Security Alert System
SSP	Ship Security Plan
TSS	Traffic Separation Scheme
UKMTO	United Kingdom Maritime Trade Operations
VDR	Vessel Data Recorder
VHP	Vessel Hardening Plan
VMS	Vessel Monitoring System
VPD	Vessel Protection Detachment
VRA	Voluntary Reporting Area
WBIED	Water-Borne Improvised Explosive Devices

Annex I

Supporting organisations

I.1 BMP5 Signatories

BIMCO

BIMCO is the world's largest international shipping association, with around 2,000 members in more than 120 countries, representing 56% of the world's 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.

www.bimco.org

CDI

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 industy 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

CLIA

Cruise Lines International Association (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.

www.cruising.org

ICS International Chamber of Shipping

The **International Chamber 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

IFSMA

The **International Federation of Shipmasters' Associations (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.

www.ifsma.org

IGP&I Clubs

Thirteen principal underwriting associations "the Clubs" comprise the **International Group of P&I Clubs (IGP&I)**. 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.

www.igpandi.org

IMCA

The International Marine Contractors Association (IMCA) is a leading trade association representing the vast majority of contractors and the associated supply chain in the offshore marine construction industry worldwide. We have a membership of 800 companies including contractors, suppliers, oil & gas companies, marine renewable energy companies and numerous non-governmental organisations (NGOs).

www.imca-int.com

INTERCARGO

The **International Association of Dry Cargo Shipowners (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.

www.intercargo.org

InterManager

InterManager is the international trade association for the ship management industry established in 1991. It is the voice of ship management and the only organisation dedicated to representing the ship management and crew management industry. In today's global shipping industry InterManager works for the needs of like-minded companies in the ship and crew management sector, who all have the welfare of seafarers at their heats. InterManager acts as a forum to share best practices and bring about positive change. An internationally-recognised organisation, InterManager represents its members at international level, lobbying on their behalf to ensure their views are taken into account within the worldwide maritime industry.

www.intermanager.org

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.

www.imec.org.uk

International Transport Workers' Federation

The **International Transport Workers' Federation (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 the 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

IPTA

The **International Parcel Tankers Association (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

ISWAN

The **International Seafarers Welfare and Assistance Network (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 PandI 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

Joint Hull Committee and Joint War Committee

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.

The Mission to Seafarers

The Mission to Seafarers is the largest provider of port-based welfare services, providing 200 port chaplains and 121 seafarers' centres across 50 countries. In addition to our services of free Wi-Fi, respite and transportation, all chaplains are trained in post-trauma counselling and are able to provide immediate support post attack or release, as well as connect with relevant professional services in a seafarer's home country. We run family support networks in the Philippines, Myanmar, Ukraine and India offering access to education, training and medical and legal services. The Mission to Seafarers is pleased to support the creation of BMP5 and the associated resources and commends their use to all maritime personnel.

www.missiontoseafarers.org

OCIMF

The **Oil Companies International Marine Forum (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

Sailors' Society

Sailors' Society is the world's oldest maritime welfare organisation caring for seafarers and their families across the globe.

The charity works in ports across 30 countries and has projects ranging from medical centres to building boats to get children safely to school.

Our renowned Crisis Response Network helping victims of trauma at sea is run across Asia, Europe and Africa with plans to extend further.

Trained chaplains offer 24-hour support to victims of piracy, kidnapping and natural disasters and come alongside survivors and loved ones with psychological and financial help for as long as needed.

www.sailors-society.org

SIGTTO

The **Society for International Gas Tanker and Terminal Operators (SIGTTO)** 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.

www.sigtto.org

World Shipping Council

The **World Shipping Council (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

I.1 Naval/military/governmental organisations

CGPCS

The **Contact Group on Piracy off the Coast of Somalia (CGPCS)** was established on 14 January 2009, in accordance with UN Security Council Resolution 1851. This ad hoc international forum brings together more than 60 countries, regional and international organisations, all working together towards the prevention of piracy off the coast of Somalia.

The CGPCS coordinates political, military and non-governmental efforts to combat piracy, ensures that pirates are brought to justice and support local governments to develop sustainable maritime security capabilities. The group's approach focuses on informality, inclusion and multi-stakeholder representation and is an attempt to find innovative solutions outside of formal international organisations.

Combined Maritime Forces

Combined Maritime Forces (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.

EU NAVFOR

MSCHOA

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 the **European Union Naval Force (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.

The **Maritime Security Centre Horn of Africa (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.

http://eunavfor.eu

www.mschoa.org

IMB Piracy Reporting Centre

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 incidents 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

Information Fusion Centre

The **Information Fusion Centre (IFC)**, based in Singapore, serves as the regional Maritime Security (MARSEC) information-sharing hub. It has linkages with more than 70 regional and extra-regional Operational Centres (OPCENs) from navies and law enforcement agencies in 39 countries, as well as linkages with the shipping industry. It is also the only centre in the Asia-Pacific with International Liaison Officers (ILOs) from 16 countries.

The IFC collates and analyses relevant information to produce accurate, timely and actionable products, which enable its partners to respond to MARSEC incidents in good time. It also provides practical and useful information on MARSEC trends, incidents and best practices to the shipping industry. IFC also administers the Voluntary Community Reporting (VCR) for merchant vessels to report anomalies and incidents, enabling community contribution to Safe and Secure Seas for All.

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 dlMTSOPSupport@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 190 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.

NCAGS

The **Naval Cooperation & Guidance for Shipping (NCAGS)** mission is to facilitate the exchange of information between the United States Navy, Combined Maritime Forces, and the commercial maritime community in the United States Central Command's (CENTCOM) Area of Responsibility. NCAGS operates as a conduit for information focused on the safety and security of shipping and is committed to assisting all members of the commercial maritime community. To help combat piracy, NCAGS serves as a secondary emergency point of contact for mariners in distress (after UKMTO) and also disseminates transit guidance to the maritime industry. NCAGS disseminates guidance to merchant shippers via briefings, website, email, and duty phone concerning Naval Exercises, Boardings, Aids to Navigation, Environmental Issues, MEDEVAC Assistance, Security and Augments, Regional Search and Rescue Centres.

UKMTO

UK Maritime Trade Operations (UKTMO) 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 UKMTO please contact:

Emergency Telephone Numbers: +44 (0)2392 222060 or +971 5055 23215

e-mail: watchkeepers@ukmto.org Web: **www.ukmto.org**

ANNEX 2

Annex J

Voyage reference card

Understand the threat

- Get threat information.
- Review guidance.
- Review Rules for the Use of Force.

Assess the risk

- Conduct risk assessment.
- Identify ship protection measures.

Protect the ship and crew

- Harden the ship.
- Test critical equipment.
- Brief/train the crew.
- Extra lookout/radar watch.
- Control access.
- Follow military advice.

Do NOT be alone

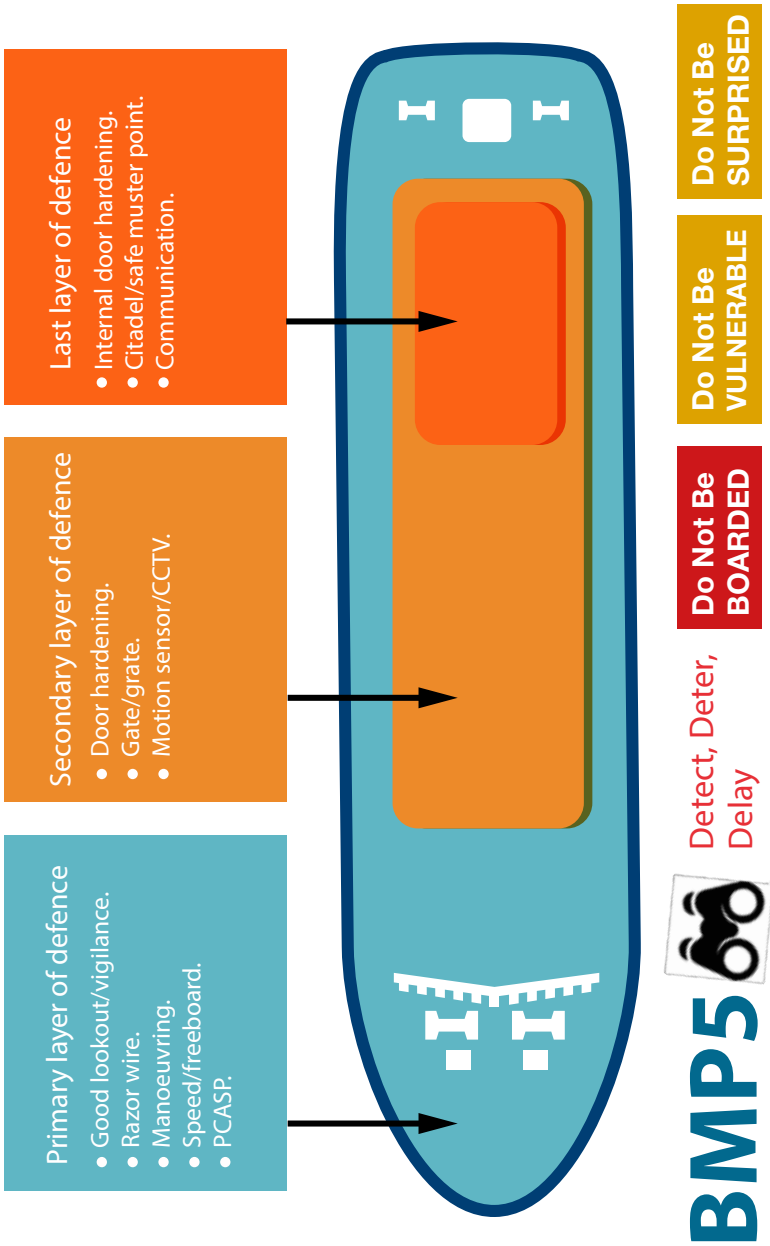
- Report to UKMTO.
- Register with MSCHOA.
- Report suspicious activity.
- Report incidents.
- Send DISTRESS if attacked.

UKMTO
+44 (0) 2392 222060
watchkeepers@ukmto.org

MSCHOA
+44 1923 958545
www.mschoa.org

Cooperate with:

- Other shipping and military forces.
- Local law enforcement.
- Welfare providers.


Primary layer of defence
• Good lookout/vigilance.
• Razor wire.
• Manoeuvring.
• Speed/freeboard.
• PCASP.
Secondary layer of defence
• Door hardening.
• Gate/grate.
• Motion sensor/CCTV.
Last layer of defence
• Internal door hardening.
• Citadel/safe muster point.
• Communication.
BMP5
Detect, Deter, Delay
Do Not Be BOARDED
Do Not Be VULNERABLE
Do Not Be SURPRISED

ANNEX 2

Guidelines for Owners, Operators and Masters for protection against piracy and armed robbery in the Gulf of Guinea region (Version 3, June 2018)

To be read in conjunction with the Global Counter-Piracy Guidance for Companies, Masters and Seafarers (GCPG).

Issued by ICS, BIMCO, Intercargo, IG P&I, INTERTANKO, InterManager, OCIMF

1. Introduction

Piracy and armed robbery in the Gulf of Guinea region is an established criminal activity and is of serious concern to the maritime sector.

2. Area for consideration

Attackers in the Gulf of Guinea region are flexible in their operations so it is difficult to predict a precise area where a ship might fall victim to an attack. For the purpose of this guidance the area off the coasts of Ghana, Nigeria, Togo, Cameroon, and Benin can be regarded as an area in which this guidance should be applied. Attacks have occurred from as far south as Angola and as north as Sierra Leone.

In addition, the LMA Joint War Committee defines the following "Listed Areas for Hull War, Piracy, Terrorism and Related Perils":

- The territorial waters of Benin, Togo and Nigeria, plus
- Nigerian Exclusive Economic Zone north of latitude 3º N, plus
- Beninese Exclusive Economic Zones north of latitude 3º N plus.
- Togolese Exclusive Economic Zone north of latitude 3º N.

The LMA Joint War Committee listed areas should be checked regularly for changes www.lmalloyds.com/lma/jointwar

3. Threat and Risk Assessment

For the purpose of identifying suitable measures of prevention, mitigation and recovery in case of piracy, ship and voyage specific threat and risk assessment as recommended in Section 4 of GCPG should be carried out prior to entering the area described in Section 2 above . Not unlike the Ship Security Assessment described in the ISPS Code, the risk assessment should include, but may not be limited to, the following:

- The threat (who are the attackers, what do they want to achieve, how do they attack, how do they board, which weapons do they use etc.?)
- Background factors shaping the situation (visibility, sea-state, traffic patterns e.g. other commercial ships, fishermen and human traffickers etc.)

- Possibilities for cooperation with military (escorting, employment of Vessel Protection Detachments, registering with authorities etc.)
- The ship's characteristics/vulnerabilities/inherent capabilities to withstand the threat (freeboard, speed, general arrangement etc.)
- Ship's procedures (drills, watch rosters, chain of command, decision making processes etc.)

In addition to the information found in this document, supplementary information about the characteristics of the threat and regional background factors may be sought from regional reporting centres, Shipping Association websites, the International Maritime Bureau (IMB), commercial intelligence providers or local sources such as ships' agents.

As described in the GCPG, the risk assessment should take into consideration any statutory requirements, in particular those of the flag state and/or the coastal state. Other requirements dictated by company and insurance policies should also be taken into consideration.

Much of this risk assessment already exists in the GCPG since it provides an overall list of which actions to take to defend against attack. However, the guidance in the GCPG must be developed into specific actions and mitigation measures to apply on a ship-by-ship and voyage-by-voyage basis. For example, many attacks in the Gulf of Guinea region occur whilst ships are at anchor or drifting, in which case the GCPG self-defence measures like "evasive maneuvering" are not readily applicable. Thus, the risk assessment must reflect the prevailing characteristics of the specific voyage and ship, and not just be a repetition of advice relating to a different geographical region and a different attacking modus operandi. Detailed guidance on preparing risk assessments can be found from a variety of sources including the ISPS code.

4. Typical Attacks

Attacks within the Gulf of Guinea are varied, and include armed robbery of crew and ship's property, cargo theft and kidnap for ransom. Generally speaking, attacks in the Gulf of Guinea can be very violent and can be split broadly into the following categories:

- Armed Robbery – In general this is opportunistic, is often violent, and occurs where ships are approaching, drifting, anchored off and berthed alongside at ports. For the most part the intention is to take valuables from the safe, IT equipment, and personal effects.
- Cargo theft – This occurs throughout the area described with ships hijacked in anchorages and whilst underway further offshore. In the main it is related to product and chemical tankers but there are also attacks on general cargo carriers. Ships are hijacked for several days and cargo is transferred to a smaller ship. These incidents are well-organized, often involving a criminal element with commercial interests ashore. Cargo thefts have demonstrated that attackers often have maritime knowledge allowing them to disable communications, operate the cargo system, etc.
- Kidnapping – All seafarers and all types of ships are at risk. Instances of ships being attacked and seafarers taken ashore for ransom remain relatively common. The methodology is to take 4 to 5

seafarers – often the Master and Chief Engineer -as they command higher ransoms. However, there have been cases where 10 or more crew have been seized.

Attacks in the Gulf of Guinea region usually involve approaches made by high-powered speedboats. The use of motherships is not widespread, although there is evidence that small cargo ships and fishing ships that have already been hijacked have been used to launch attacks against larger merchant ships.

The risk of an attack is higher when the ship is at anchor or is approaching or drifting off a port e.g. close to pilot station. Another vulnerable situation arises when STS operations and the two ships are adrift and moored alongside each other.

For the tanker sector, cargo theft results in stolen oil products being sold in the region. For the dry cargo and other sectors, violent robbery is more common. Attacks, both outside and inside territorial waters, appear to be the result of well executed planning, with particular products such as gasoil or gasoline being targeted in well-coordinated operations. Companies and ships operating regularly in the region are likely to be at increased risk of falling subject to intelligence collection operations and subsequent attack.

5. Ship Movement Reporting Procedures

Although this may change in the future, at present the Yaoundé reporting framework is not fully operational, with voluntary ship movement and reporting procedures handled by the MDAT-GoG. Masters have a number of options for reporting incidents and particularly:

<u>Maritime Domain Awareness for Trade – Gulf of Guinea (MDAT-GoG):</u>

MDAT-GoG is a service operated by the French and UK navies from centres in Brest, France, and Portsmouth, UK and aims to develop, maintain and share details of the maritime domain picture of the waters off Africa's western seaboard. The MDAT-GoG administers a Voluntary Reporting Area (VRA) scheme under which merchant ships are encouraged to report position information while operating in the VRA.

The VRA, as shown on Admiralty Chart Q6114, has been issued to clearly define an internationally recognized area, so ship operators and ships transiting, trading or operating in West Africa can join a trusted reporting scheme. The provision of Admiralty Chart Q6114 to all ships operating in the VRA is strongly recommended.

Suspicious activity and incidents reported to MDAT-GoG by shipping in the VRA, using the forms on the Chart and repeated at Annex B, assist in the creation of a detailed and accurate regional maritime domain picture. The analysis is used to produce security recommendations that are shared with seafarers, ship operators and law enforcement agencies to enhance risk awareness and improve incident response.

The MDAT-GoG provides a 24-hour manned service of military experts. The MDAT-GoG receives reports, shares important updates and provides guidance on ship operating patterns and security risks with the Gulf of Guinea maritime community.

- The MDAT-GoG has no influence over the deployment of local military assets to assist merchant ships which are attacked but is linked with national and regional maritime operations centres and may be able to help direct them to the scene of an incident.
- Dedicated naval staff collate data from a variety of sources to aid their understanding of the maritime environment. The voluntary position reports from ships operating within the VRA are an important

input to greater understanding of maritime activity - the information reported is used to inform other regional governmental organizations and inform recommendations to enhance security planning, incident response and investigations.

Owners and operators should bring this reporting scheme to the attention of their ships to encourage ships entering the VRA to report, make daily reports during transit and log a departure report when leaving. The contact details and details of the report format are shown at Annex A.

Reporting:

Ships are encouraged to send regular reports, using the MDAT-GoG reporting forms as below:

WHEN	WHAT
On entering the VRA	Initial Report
Daily**	Daily Position Report
On Departing the VRA	Final Report
By Exception	By Exception Report

** At 0800 if convenient to daily routine**

How to Report?

The MDAT-GoG reporting forms (see Annex B), should be used to make the reports described above.

Email is the preferred method of communication but alternatively telephone, (see Annex A for contact details).

Regional Maritime Rescue Coordination Centres:

These are established at Monrovia and Lagos and are important points for safety reporting. See Section 13 for more details.

International Maritime Bureau (IMB):

Ships are encouraged to report all incidents to the IMB reporting centre in order to accurately reflect the number and types of incident. See Section 13

Yaoundé Framework

The Yaoundé framework is establishing a number of other reporting centres. It is expected that the Inter-regional Coordination Centre in Yaoundé will soon be operational.

Individual flag states may well have their own national ship movement reporting procedures. Any flag state reporting requirements should be clarified and complied with.

The above guidance is the best available at the time of publication but is likely to change as new reporting centres become operational and regional coordination and cooperation increases. Owners and Operators should monitor the developing situation in order to ensure that ships operating in the region are aware of reporting options available to them. It is essential that each and every incident is reported in order to maintain pressure on coastal states to meet their obligations under UNCLOS and encourage the international community to support infrastructure and capacity building in the region.

6. Company Planning

Company planning procedures outlined in Section 5 of GCPG should be applied in the Gulf of Guinea region. The following important advice should be noted:

- Communications with external parties should be kept to a minimum, with close attention paid to organizing rendezvous points and waiting positions. For e-mail correspondence to Agents, Charterers, Chandlers etc. it is strongly recommended that address lists are controlled and that information within the e-mail is concise, containing the minimum that is legally required in order to fulfil requirements or contractual obligations.
- Contractual arrangements should be put in place with a view to keeping ships out of harm's way.
- Know your agents and avoid or minimize requirements where possible. Unnecessary interaction with other parties creates opportunities for information regarding the ship's position to be compromised.
- If the ship trades regularly in the region it is recommended to occasionally alter arrangements to make it harder for criminals to predict where operations might take place.

In terms of the availability of armed escort ships, the Nigerian Navy are known to offer licenses to certain companies to employ naval personnel on board their escort ships.

7. Master's Planning

Many of the Master's planning procedures described in Section 6 of GCPG also apply to the Gulf of Guinea, although there are no Group Transit schemes or national convoys. Given the modus operandi of the attackers operating in the Gulf of Guinea region, the Master should plan according to the following:

- Rendezvous - Where possible, avoid waiting and slow steaming. Consider offering several alternative rendezvous points and advise rendezvous points at the last minute. If waiting, keep well off the coast (up to 200nm). Do not give away waiting positions. Do not drift and keep engines ready for immediate maneuvers.
- Anchoring - Where practicable, a prolonged stay at anchorage is to be avoided.
- Minimize use of VHF and use e-mail or secure satellite telephone instead. Where possible only answer known or legitimate callers on the VHF, bearing in mind that imposters are likely and may even appear in uniform.
- Within anchorages and ports, the greatest risks of piracy and robbery are at night due to criminals being able to operate under the cover of darkness.
- Further offshore, attacks can occur at any time of day or night, as pirates are able to operate more freely further away from military forces and law enforcement.

- For ships approaching pilot stations, curfew times at anchorages and on rivers should be factored into all planning to ensure minimal waiting time drifting or at anchor. Where possible, operations should start and end during daylight hours.

8. Ship Protection Measures

The ship protection measures described in Section 7 of GCPG also apply in the Gulf of Guinea region. When STS operations are expected to be conducted, extra attention should be paid to the use of physical protection measures. Although barbed wire can potentially make it very difficult to complete an STS operation, other protection measures should be considered to protect the ship from attack in these cases.

- Ship hardening can be effective in this region and a moving ship also makes an effective deterrent.
- During STS operations or when adrift, equipment such as fenders, anchor chains and hawse pipes can potentially provide a vulnerable point of access for attackers, and entry should be physically blocked.
- Attackers detect and target ships by sight and by the use of AIS. Therefore limit the use of lighting at night and reduce the power of AIS. Unfortunately, this has a major drawback in that it may reduce the likelihood of an intervention by "friendly forces" if attacked. Consequently, **AIS must be switched on immediately if the ship is boarded**.
- The use of citadels or safe muster points is an owner's/master's choice but it should be borne in mind that their successful use in the Indian Ocean was predicated upon their being a strong chance of a Naval Intervention. The principles of citadel construction and use are outlined in GCPG. Given the levels of violence perpetrated by attackers, and if control of the engines can be maintained from the citadel, many think that this option is the safest and also one that prevents the ship from maneuvering in order to prevent cargo theft. If a citadel is constructed, ship operators should make sure that it includes VHF communication as this is often the only available means of communication with regional naval ships in the event of a military response.
- Owners should consider the placement of hidden position transmitting devices as one of the first actions of attackers is to disable all visible communication and tracking devices and aerials.

9. Attack

The guidelines in GCPG Section 8 are applicable.

In the event of an attack in the Gulf of Guinea region, the best way of alerting the local authorities of an attack is via the MDAT-GoG and by sending out a distress message. Maintain contact with the MDAT-GoG preferably by telephone for as long as it is safe to do so. On receipt of information in relation to an attack, the MDAT-GoG will inform the appropriate national maritime operations centre and local authorities and will ensure all other ships in the immediate vicinity are aware of the event.

The following list of actions below should be considered if an attack is imminent:

- If underway speed should be increased as much as possible to open the distance between

the ship and the attackers. Try to steer a straight course to maintain maximum speed. Consider evasive actions if the circumstances dictate.

- Initiate the ship's pre-prepared emergency procedures.
- Activate the Emergency Communication Plan.
- Sound the emergency alarm and make an announcement in accordance with the Ship's Emergency Plan.
- Report the attack as soon as possible to MDAT-GoG by phone and follow up with call to the Company Security Officer if the situation permits.
- Activate the Ship Security Alert System (SSAS) which will alert your CSO and Flag State. Make a 'Mayday' call on VHF Ch. 16.
- Send a distress message via the Digital Selective Calling system (DSC) and Inmarsat-C, as applicable.
- Ensure that the Automatic Identification System (AIS) is switched ON.
- All crew, except those required on the bridge or in the engine room, should move to the Safe Muster Point or Citadel if constructed. Any Safe Muster Point should provide the crew with as much protection as possible should the attackers get close enough to use firearms.
- If possible, alter course away from the approaching craft. When sea conditions allow, consider altering course to increase an approaching craft's exposure to wind/waves.
- Activate water spray and other self-defensive measures.
- Confirm external doors and, where possible, internal public rooms and cabins, are fully secured. If possible pull-up external ladders and fenders.
- Place the ship's whistle/foghorn/alarm on Auto to demonstrate to any potential attacker that the ship is aware of the attack and is reacting to it.

If communication is lost or difficult alternative options include:

- The Regional Maritime Rescue Coordination Centre (RMRCC) in Lagos; or
- The RMRCC Monrovia if in the western extremities of the GoG.

The Lagos centre covering all coastal states from Benin to the DRC is run by the Nigerian Maritime Administration and Safety Agency (NIMASA) and can be contacted via details shown in Section 13 of this Guidance. The Monrovia centre covering the area from Guinea to Ghana is run by the Liberian Maritime Administration and can be contacted via details at Section 13.

When contacted, the Lagos and Monrovia RMRCC will alert the military and/or coast guard forces in the region who will initiate a response if the necessary resources are available at the time of the alert.

10. If Attackers Take Control

The advice in Section 9 of GCPG is also applicable. MDAT-GoG, Lagos RMRCC or Monrovia RMRCC should be contacted.

As previously mentioned the attackers operating in the Gulf of Guinea region often use violence in order to subdue the crew. Therefore it is extremely important not to engage in a fight with the attackers, because this will entail great risk of the crew getting hurt or killed.

Violent shipboard robberies can take place as a result of a previously unsuccessful attack on another ship. Therefore:

- Great care needs to be taken if your ship is boarded, as life is little valued by robbers. Compliance/submission to attackers is essential once they have taken control of a ship.
- Generally minimizing cash carried will make ships less attractive in the longer run.

Kidnap and Ransom in the Gulf of Guinea region is an established practice. Experience shows attackers will board a ship and loot the ship's stores and steal personal belongings. Once this has been done they may kidnap key individuals e.g. the Master and Chief Engineer.

Kidnap can serve two key purposes for the attackers:

- Help the attackers escape. The presence of hostages may reduce the likelihood of security forces to engage in a firefight and;
- For ransom. To maximize their profits from the attack or hijack.

Each company or organization will have a policy in place to cover the eventualities of Kidnap and Ransom.

11. In the Event of Military Action

Section 8.7 of the GCPG applies.

12. Post Incident Reporting

All piracy incidents ought to be reported to the IMB in accordance with Annex A to this Guidance (for contact details, see Section 13).

In addition, incidents in the GoG should be reported to Interpol via the West African Police Information System (WAPIS) Regional Bureau in Abidjan. (see Section 13 for contact details)

The relevant reporting format can be found in Annex B.

13. MDAT-GoG Contact details

- Website: development in progress

E-mail: watchkeepers@mdat-gog.org Telephone (24hrs): +33(0)2 98 22 88 88

INTERPOL Command and Coordination Centre

- Website: www.interpol.int
- E-mail: os-ccc@interpol.int
- Telephone (24hrs): +33 (0) 47244 7676

Lagos Regional Maritime Rescue Coordination Centre (RMRCC)

NIGERIA

- Telephone (24hrs): +234 (1) 730 6618
- The Lagos MRCC covers nine countries (Benin, Cameroon, Republic of Congo, the Democratic Republic of Congo, Equatorial Guinea, Gabon, Nigeria, São Tomé & Príncipe and Togo).

Monrovia Regional Maritime Rescue Coordination Centre (RMRCC)

LIBERIA

- INMARSAT C Terminals: # 580-460173-111 AOR-E
- INMARSAT C Terminals: # 580-460199-019 AOR-W
- International Fax: # (+231) 2430-0011
- International Landline: # (+231) 770-092229
- International Cellular & SMS: # (+231) 573-0144
- VHF-DSC Radio
- Monrovia covers the territorial waters of Liberia and her four neighboring countries - Guinea, Ghana, Liberia, Sierra Leone, and Cote d'Ivoire.

International Maritime Bureau – IMB Piracy Reporting Centre (IMB PRC)
ICC IMB (Asia Regional Office),
PO Box 12559,
Kuala Lumpur,
50782,
Malaysia.

Tel: + 60 3 2078 5763
Fax: + 60 3 2078 5769
E-mail: imbkl@icc-ccs.org / piracy@icc-ccs.org
24 Hour Anti Piracy HELPLINE Tel: + 60 3 2031 0014

ANNEX A

MDAT-GOG REPORTING FORMS

Once a ship has transmitted an Initial Report to MDAT-GoG, MDAT-GoG will reply and request that Daily Reports be transmitted. Upon exiting the VRA, ships should complete and transmit a Final Report. The following forms are used:

- Initial Report Format
- Daily Report Format
- Final Report Format
- By Exception Report Format.

Masters and operators should check either by email to the Watchkeeper or check with the MDAT-GoG website for the latest information regarding the Voluntary Reporting Area. The MDAT-GoG accepts forms by e-mail.

MDAT-GoG Ship Position Reporting Form - Initial Report

01	Ship Name	
02	Flag	
03	IMO Number	
04	INMARSAT Telephone Number	
05	Time & Position	
06	Course	
07	Passage Speed	
08	Freeboard	
09	Cargo	
10	Destination and Estimated Time of Arrival (including anchorages etc)	
11	Name and contact details of Company Security Officer	
12	Nationality of Master and Crew	
13	Armed/unarmed security team embarked	

MDAT-GoG Ship Position Reporting Form - Daily Position Report

01	Ship's name	
02	Ship's Call Sign and IMO Number	
03	Time of Report in UTC	
04	Ship's Position	
05	Ship's Course and Speed	

06	Any Other Important Information	

MDAT-GoG Ship Position Reporting Form - Final Report

01	Ship's name	
02	Ship's Call Sign and IMO Number	
03	Time of Report in UTC	
04	Port or position when leaving the VRA	

MDAT-GoG By Exception Report (Suspicious Activity)

01	Own Ship name	
02	Ship's Call Sign and IMO Number	
03	Time of Report in UTC	
04	Own Ship Position	
05	Own Ship Course and Speed	
06	Sightings of Illegal Unlawful Unregulated (IUU) fishing or other assessed illegal activity. Time, Position, brief description of craft and activity witnessed	

ANNEX B

PIRACY ATTACK REPORT, SHIP

General Details

01 Name of Ship:

02 IMO No:

03 Flag:

04 Call Sign:

05 Type of Ship:

06 Tonnages:
GRT:
NRT:
DWT:

07 Owner's (Address & Contact Details):

08 Manager's (Address & Contact Details):

09 Last Port/Next Port:

10 Cargo Details: (Type/Quantity)

Details of Incident

11 Date & Time of Incident:
LT UTC

12 Position:
Lat: (N/S)
Long: (E/W)

13 Nearest Land Mark/Location:

14 Port/Town/Anchorage Area:

15 Country/Nearest Country:

16 Status (Berth/Anchored/Steaming):

17 Own Ship's Speed:

18 Ship's Freeboard During Attack:

19 Weather During Attack (Rain/Fog/Mist/Clear/etc, Wind (Speed and Direction), Sea/Swell Height):

20 Types of Attack (Boarded/Attempted):

21 Consequences for Crew, Ship and Cargo:
Any Crew Injured/Killed:
Items/Cash Stolen:

22 Area of the Ship being Attacked:

23 Last Observed Movements of Pirates/Suspect Craft:

24 Type of vessel (Whaler, Dhow, Fishing Vessel, Merchant Vessel)

25 Description of vessel (Colour, Name, Distinguishing Features)

26 Course and Speed of vessel when sighted

Details of Raiding Party

27 Number of Pirates/Robbers:

28 Dress/Physical Appearance:

29 Language Spoken:

30 Weapons Used:

31 Distinctive Details:

32 Craft Used:

33 Method of Approach:

34 Duration of Attack:

35 Aggressive/Violent:

Further Details

36 Action Taken by Master and Crew and its effectiveness:

37 Was Incident Reported to the Coastal Authority? If so, to whom?

38 Preferred Communications with Reporting Ship:
Appropriate Coast Radio Station/HF/MF/VHF/INMARSAT
IDS (Plus Ocean Region Code)/MMSI

39 Action Taken by the Authorities:

40 Number of Crew/Nationality:

41 Please attach with this Report – A Brief Description/Full Report/Master – Crew Statement of the Attack/Photographs taken if any.

42 Details of Self Protection Measures.