ST. VINCENT AND THE GRENADINES

MARITIME ADMINISTRATION

CIRCULAR N° APIR 002 Rev. 4

PIRACY AND ARMED ROBBERY AGAINST SHIPS

MSC.1/Circ.1333 Rev 1, MSC/Circ.1334 and MSC.1/Circ.1601/Rev.1

TO: SHIPOWNERS & SHIPS' OPERATORS & MANAGERS, MASTERS AND THE SHIPBOARD PERSONNEL EMPLOYED OR ENGAGED ON SVG VESSELS

APPLICABLE TO: ALL SHIPS
ENTRY INTO FORCE: DATE OF CIRCULAR

22 November 2021

In view of the increasing occurrences of piracy and armed robbery against vessels, this Administration brings to the attention of the Shipowners, Ships' Operators and Managers, Masters and the Shipboard Personnel employed or engaged on Saint Vincent and the Grenadines vessels, the MSC.1/Circ.1601/Rev.1, which is annexed to this circular.
They are required to act in accordance with the Annexes of the circular as follows:

- 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.

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.

Annexes to this Circular:

MSC.1/Circ.1333 Rev 1,
MSC/Circ.1334,
MSC.1/Circ.1601/Rev.1

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.1333/Rev.1
12 June 2015

PIRACY AND ARMED ROBBERY AGAINST SHIPS

Recommendations to Governments for preventing and suppressing piracy and armed robbery against ships

1 The Maritime Safety Committee, at its ninety-fifth session (3 to 12 June 2015), revised MSC.1/Circ.1333 by incorporating provisions for the establishment of a national point of contact for communication of information on piracy and armed robbery to the Organization given in the annex.

2 Member Governments, in particular those within areas identified as affected by acts of piracy and armed robbery against ships, are recommended to take any necessary action to implement, as appropriate, the recommendations given in the annex.

3 Member Governments are also recommended to bring this circular and MSC.1/Circ.1334 to the attention of all national agencies concerned with anti-piracy and anti-armed robbery activities, shipowners, ship operators, shipping companies, shipmasters and crews.

4 This circular revokes MSC.1/Circ.1333.

***

ANNEX

RECOMMENDATIONS TO GOVERNMENTS FOR PREVENTING AND SUPPRESSING PIRACY* AND ARMED ROBBERY[1] AGAINST SHIPS

Piracy and armed robbery against ships

1 Before embarking on any set of measures or recommendations, it is imperative for governmental or other agencies concerned to gather accurate statistics of the incidents of piracy and armed robbery against ships, to collate these statistics under both type and area and to assess the nature of the attacks with special emphasis on types of attack, accurate geographical location and *modus operandi* of the wrongdoers and to disseminate or publish these statistics to all interested parties in a format that is understandable and usable. Advanced intelligence could also prove useful in obtaining information to Governments in order to be able to act in a coordinated manner even before an attack occurs. Based on the statistics of the incidents and any intelligence of piracy and armed robbery against ships Governments should issue to ships entitled to fly their flag, as necessary, advice and guidance on any appropriate additional precautionary measures ships may need to put in place to protect themselves from attack. Governments should involve representatives of shipowners and seafarers in developing these measures to prevent and suppress piracy and armed robbery against ships.

2 In any ongoing campaign against piracy and armed robbery, it is necessary, wherever possible, to neutralize the activities of pirates and armed robbers. As these people are criminals under both international law and most national laws, this task will generally fall to the security forces of the States involved. Governments should avoid engaging in negotiations with these criminals and seek to bring perpetrators of piracy and armed robbery against ships to justice. Negotiating with criminals in a case regarding hijacking of a ship may encourage potential perpetrators to seek economic revenue through piracy.

---

* The following definition of piracy is contained in article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS) (article 101):

"Piracy consists of any of the following acts:

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

1 The Sub-regional meeting on piracy and armed robbery against ships in the Western Indian Ocean, Gulf of Aden and Red Sea area, held in Dar es Salaam, United Republic of Tanzania, from 14 to 18 April 2008, agreed to modify this definition. Consistent with the ReCAAP Agreement, the "private ends" motive has been added to the definition. The formulation "within internal waters, archipelagic waters and territorial sea" replaced "within a State's jurisdiction". The new formulation reflects the views of France, supported by other States participating in the meeting, that the definition for armed robbery against ships should not be applicable to acts committed seaward of the territorial sea. The new definition reads: "Armed robbery against ships" means any unlawful act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, 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.

Self-protection

3 Ships can and should take measures to protect themselves from pirates and armed robbers. These measures are recommended in MSC.1/Circ.1334. While security forces can often advise on these measures, and flag States are required to take such measures as are necessary to ensure that owners and masters accept their responsibility, ultimately it is the responsibility of owners, companies, ship operators and masters to take seamanlike precautions when their ships navigate in areas where the threat of piracy and armed robbery exists. Flag States should make shipowners/companies aware of any United Nations Security Council, International Maritime Organization (IMO), or any other United Nations resolutions on piracy and any recommendations therein relevant for the shipowner, ship operator, the master and crew when operating in areas where piracy or armed robbery against ships occur.

4 With respect to the carriage of firearms on board, the flag State should be aware that merchant ships and fishing vessels entering the territorial sea and/or ports of another State are subject to that State's legislation. It should be borne in mind that importation of firearms is subject to port and coastal State regulations. It should also be borne in mind that carrying firearms may pose an even greater danger if the ship is carrying flammable cargo or similar types of dangerous goods.

Non-arming of seafarers

5 For legal and safety reasons, flag States should strongly discourage the carrying and use of firearms by seafarers for personal protection or for the protection of a ship. Seafarers are civilians and the use of firearms requires special training and aptitudes and the risk of accidents with firearms carried on board ship is great. Carriage of arms on board ships may encourage attackers to carry firearms or even more dangerous weapons, thereby escalating an already dangerous situation. Any firearm on board may itself become an attractive target for an attacker.

Use of unarmed security personnel

6 The use of unarmed security personnel is a matter for individual shipowners, companies, and ship operators to decide. It should be fully acceptable to provide an enhanced lookout capability this way.

Use of privately contracted armed security personnel

7 The use of privately contracted armed security personnel on board ships may lead to an escalation of violence. The carriage of such personnel and their weapons is subject to flag State legislation and policies and is a matter for flag States to determine in consultation with shipowners, companies, and ship operators, if and under which conditions this will be allowed. Flag States should take into account the possible escalation of violence which could result from carriage of armed personnel on board merchant ships, when deciding on its policy.

Military teams or law enforcement officers duly authorized by Government

8 The use of military, or law enforcement officers duly authorized by the Government of the flag State to carry firearms for the security of the ship is a matter for the flag State to authorize in consultation with shipowners, companies, and ship operators. Flag States should provide clarity of their policy on the use of such teams on board vessels entitled to fly their flag.

Action plans

9 The coastal State/port State should develop action plans detailing how to prevent such an attack in the first place and actions to take in case of an attack. Coastal States should consider their obligations under SOLAS regulation XI-2/7 on Threats to ships which requires, inter alia, where a risk of attack has been identified, the Contracting Government concerned shall advise the ships concerned and their Administrations of:

.1 the current security level;

.2 any security measures that should be put in place by the ships concerned to protect themselves from attack, in accordance with the provisions of part A of the ISPS Code; and

.3 security measures that the coastal State has decided to put in place, as appropriate.

Also, due to the possibility of collision or grounding of a ship as a result of an attack, the coastal State/port State will need to coordinate these action plans with existing plans to counter any subsequent oil spills or leakages of hazardous substances that the ship or ships may be carrying. This is especially important in areas of restricted navigation. The coastal State/port State should acquire the necessary equipment to ensure safety in waters under their jurisdiction.

10 Flag States should develop action plans detailing the response to be taken on the receipt of a report of an attack and how to assist the owners, companies[1], managers and operators of a ship in case of a hijacking. A point of contact through which the ships entitled to fly their flag may request advice or assistance when sailing in waters deemed to present a heightened threat and to which such ships can report any security concerns about other ships, movements or communications in the area, should be provided.

11 All national agencies involved in preventing and suppressing piracy and armed robbery against ships should take appropriate measures for the purpose of maximizing efficiency and effectiveness and, at the same time, minimizing any relevant adversity. The coastal State/port State should also establish the necessary infrastructure and operational arrangements for the purpose of preventing and suppressing piracy and armed robbery against ships.

12 States and relevant international organizations are encouraged to support capacity-building in areas or regions where piracy and armed robbery against ships is known to occur.[2]

13 Where ships are employed by a United Nations (UN) humanitarian programme for the delivery of humanitarian aid into areas at heightened threat, where such ships are to be escorted by warships or military aircraft, or other ships or aircraft clearly marked and identifiable as being on Government service, such escorts should be implemented in conformity with international law and United Nations resolutions. The flag State of the ship being escorted should endeavour to conclude any necessary agreements in respect of such ships entitled to fly their flag with the State(s) providing the escorts.

---

1 The term "company" is defined in SOLAS regulations IX/1 and XI-2/1.

2 The ReCAAP Information Sharing Centre (ReCAAP ISC) undertakes capacity-building initiatives to enhance the capability of ReCAAP Contracting Parties in combating piracy and armed robbery against ships in the region. The Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) is a government-to-government Agreement that addresses the incidence of piracy and armed robbery against ships in Asia. The status of ReCAAP ISC is an IGO. Further details may be found at www.recaap.org. Similar arrangements are being developed by IMO in other regions.

14 Article 100 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS) requires all States to cooperate to the fullest possible extent in the repression of piracy. In this regard, States interested in the security of maritime activities should take an active part in repression of and fight against piracy, particularly in areas where the United Nations Security Council expresses concern about the imminent threat of attacks by pirates and calls upon States to do so. This could be done by prosecuting suspected pirates, contributing to capacity building efforts and by deploying naval vessels and aircraft in accordance with international law to patrol the affected areas.

15 On communication and cooperation between various agencies, and the response time after an incident has been reported to the coastal State:

.1 an incident command system for tactical as well as operational response should be adopted in each country concerned to provide a common terminology; integrated communications; a unified command structure; consolidated action plans; a manageable span of control; designated incident facilities; and comprehensive resource management;

.2 existing mechanisms for dealing with other maritime security matters, e.g. smuggling, drug-trafficking and terrorism, should be incorporated into the incident command system in order to allow for efficient use of limited resources;

.3 procedures for rapidly relaying alerts received by communication centres to the entity responsible for action should be developed or, if existing, kept under review; and

.4 Governments should by bilateral or multilateral agreements cooperate in establishing, when appropriate, a single point of contact for ships to report piracy threats or activities in specific high threat areas.

16 It is imperative that all attacks, or threats of attacks, are reported immediately to the nearest RCC[1] or coast radio station to alert the coastal State/port State and followed up by a more detailed written report.[2] On receipt of radio reports of an attack or post attack reports, the RCC or other agency involved must take immediate action to:

.1 inform the local security authorities so that contingency plans (counter action) may be implemented;

.2 alert other ships in the area to the incident utilizing any appropriate communication means available to it, in order to create or increase their awareness; and

.3 inform the adjacent RCCs when appropriate.[3]

17 The report received by maritime Administrations may be used in any diplomatic approaches made by the flag State to the Government of the coastal State in which the incident occurred. This will also provide the basis for the report to IMO.

---

1 In the Asian region, the RCCs of some ReCAAP Contracting Parties are also the ReCAAP Focal Points. The RCCs of the coastal States disseminate information of an incident internally to their respective Focal Points, maritime authorities and law enforcement agencies, as deemed appropriate. A similar system is being developed for the Gulf of Aden and Western Indian Ocean area under the Djibouti Code of Conduct.

2 Flow diagrams for reporting incidents are attached as appendices 1 and 2.

3 A template for Ships' Message Formats is attached as appendix 4.

18 Coastal States/port States should report to IMO any act of armed robbery in their waters or acts of piracy close to their waters which have been reported to them or, if such a report has not been made, where they have information of an incident because of the geographical proximity to the incident or due to the participation in the apprehension of the perpetrators. The format presently used for reports to IMO is attached at appendix 5.

19 The recording and initial examination of reports is best done, wherever possible, by a central agency possessing the necessary skills and resources. In order to maintain the required credibility, both from Government and commercial sectors, such an agency must be accurate, authoritative, efficient and impartial in both its product and its dealings with others. It is judged that the Organization best suited to this role continues to be IMO itself, although the use of IMB's Piracy Reporting Centre in Kuala Lumpur, Malaysia, the ReCAAP Information Sharing Centre (ISC) in Singapore, the Maritime Security Centre Horn of Africa or similar arrangement, as a satellite for dissemination of information should also be considered.

20 The detailed work of assessment should be carried out by the security forces of the coastal State concerned who will probably have access to further information to complete the picture and background of the attacks and those persons responsible.

21 It is important that, once the collection and collation stages have been completed, the product be distributed to all agencies requiring that information. These agencies include the Governments of coastal States for dissemination of the information, the Governments of flag States for distributing it through maritime Administrations to shipowners/company, ship operators, to other interested Government departments and other interested agencies and relevant international organizations such as ReCAAP ISC. See appendices to this circular regarding the information sharing and incident reporting process.

22 To encourage masters to report all incidents of piracy and armed robbery against ships, coastal States/port States should make every endeavour to ensure that these masters and their ships will not be unduly delayed that the ship will not be burdened with additional costs related to such reporting, and the welfare of the crew will be taken into account.

23 Flag, port and coastal States are encouraged to enter into bilateral or multilateral agreements[1] to facilitate the investigation of acts of piracy and armed robbery against ships. States should cooperate to investigate fully all acts or attempted acts of piracy and armed robbery against ships entitled to fly their flag. Flag, port and coastal States are encouraged to inform other States and organizations of any relevant experience they may have obtained during the investigation, which other States may benefit from. States should implement the Code of Practice for Investigation of Crimes of Piracy and Armed Robbery against Ships, IMO resolution A.922(22) or subsequent resolutions.

24 On investigation into reported incidents and prosecution of pirates and armed robbers when caught:

.1 it should be firmly established which entity in each country has responsibility and legal authority for carrying out post-attack investigations, since lack of clarity during the hours after an incident may result in missed investigative opportunities and loss or deterioration of evidence;

[1] The Regional Cooperation Agreement on Combating Piracy and Armed Robbery Against Ships in Asia (ReCAAP) is an initiative that demonstrates a multilateral Government-to-Government agreement. Also see appendix 2 to this circular regarding the information sharing and incident reporting process in the Asian region.

.2 the appointed investigation agency should have personnel trained in standard investigative techniques and who are familiar with the legal requirements of the courts of their countries, as it is widely assumed that prosecution, conviction and confiscation of assets of offenders are the most effective means of discouraging would-be offenders;

.3 as offenders may be involved in other kinds of offences, piracy and armed robbery against ships should not be viewed in isolation and useful information should, therefore, be sought in existing criminal records; and

.4 systems should be in place to ensure that potentially useful information is disseminated to all appropriate parties, including investigators.

25 IMO regularly sends to coastal States reports of armed robbery stated to have been committed in their territorial waters, requesting information on the result of any investigations they have conducted. Coastal States are requested to respond to these inquiries even when they are unable to conduct an inquiry either because the incident was not reported or was reported too late for an investigation to be conducted. Any such responses should continue to be circulated to the sessions of the Committee.

National point of contact for communication of information on piracy and armed robbery to the Organization

26 Member States should communicate to the Organization the name and contact details of a national point of contact (NPoC) to interface with the Organization for piracy and armed robbery matters.

Criminal jurisdiction

27 A person apprehended at sea outside the territorial sea of any State for committing acts of piracy or armed robbery against ships, should be prosecuted under the laws of the investigating State by mutual agreement with other substantially interested States.

Substantially interested State means a State:

.1 which is the flag State of a ship that is the subject of an investigation; or

.2 in whose territorial sea an incident has occurred; or

.3 where an incident caused, or threatened, serious harm to the environment of that State, or within those areas over which the State is entitled to exercise jurisdiction as recognized under international law; or

.4 where the consequences of an incident caused, or threatened, serious harm to that State or to artificial islands, installations or structures over which it is entitled to exercise jurisdiction; or

.5 where, as a result of an incident, nationals of that State lost their lives or received serious injuries; or

.6 that has at its disposal important information that may be of use to the investigation; or

.7 that, for some other reason, establishes an interest that is considered significant by the lead investigating State; or

.8 that was requested by another State to assist in the repression of violence against crews, passengers, ships and cargoes or the collection of evidence; or

.9 that intervened under UNCLOS article 100, exercised its right of visit, under UNCLOS article 110, or effected the seizure of a pirate/armed robber, ship or aircraft under UNCLOS article 105 or in port or on land.

28 States are recommended to take such measures as may be necessary to establish their jurisdiction over the offences of piracy and armed robbery at sea, including adjustment of their legislation, if necessary, to enable those States to apprehend and prosecute persons committing such offences.

29 For visits to ports in certain countries, ships need to carry amounts of money in cash to cover disbursements and other requirements. Cash on board a ship acts as a magnet for attackers. Where the carriage of large sums of cash is necessary because of exchange control restrictions in some States, these States are urged to take a more flexible approach.

30 Flag States should require all ships operating in waters where attacks occur to have measures to prevent attacks and attempted attacks of piracy and armed robbery against ships and on how to act if such an attack or attempted attack occurs, as part of the emergency response procedures in the safety management system, or part of the ship security plan. Such measures should include a full spectrum of appropriate passive and active security measures. The ship security plan and emergency response plans should be based on a risk assessment which take into account the basic parameters of the operation including:

.1 the risks that may be faced;

.2 the ship's actual size, freeboard, maximum speed and the type of cargo, which is being transported;

.3 the number of crew members available, their capability and training;

.4 the ability to establish secure areas on board ship; and

.5 the equipment on board, including any surveillance and detection equipment that has been provided.

Ships not covered by the ISM Code or the ISPS Code should be required to take similar precautionary measures.

31 Bearing in mind that ships already have in their procedures the ability to take preventive measures, Governments should use caution when considering the use of security levels 1, 2 and 3 in the ISPS Code for piracy and armed robbery situations.

32 If at all possible, ships should be routed away from areas where attacks are known to have taken place and, in particular, seek to avoid bottlenecks. If ships are approaching ports where attacks have taken place on ships at anchor, rather than on ships underway, and it is known that the ship will have to anchor off port for some time, consideration should be given to delaying anchoring by slow steaming or longer routeing to remain well off shore thereby reducing the period during which the ship will be at risk. Such action should not affect the ship's berthing priority. Charter party agreements should recognize that ships may need to deviate away from areas where attacks occur and that ships may need to delay arrival at such ports, either when no berth is available for the ship, or offshore loading or unloading will be delayed for a protracted period.

33 **Coastal States situated in areas affected by piracy and armed robbery**

.1 in order to be able to respond, as quickly as possible, to any report from ships on piracy and armed robbery attacks, every piracy or armed robbery threat area should be adequately covered by Coast Earth Stations which are continuously operational, and which preferably are situated in the littoral State responsible for the area or in neighbouring States;

.2 neighbouring countries having common borders in areas which can be characterized as piracy and armed robbery threat areas should establish cooperation agreements with respect to preventing and suppressing piracy and armed robbery[1]. Such agreements should include the coordination of patrol activities in such areas. An example of a model agreement is attached as appendix 6;

.3 on further development of regional cooperation, a regional agreement to facilitate coordinated response at the tactical as well as the operational level should be concluded between the countries concerned:

.3.1 such an agreement should specify how information would be disseminated; establish joint command and control procedures (a regional incident command system); ensure efficient communications; set policies for joint operations and entry and pursuit; establish the links between entities involved in all maritime security matters; establish joint specialized training of and the exchange of views between investigators; and establish joint exercises between tactical and operational entities; and

.3.2 that existing agreements, bilateral or regional, be reviewed, if necessary, to allow for the extension of entry and pursuit into the territorial sea of the State(s) with which the agreement has been made and practical operational procedures which will ensure the granting of permission to extend pursuit into another jurisdiction being received by the pursuing vessel at very short notice;

.4 as piracy and armed robbery against ships is not only a regional but a global problem, the established regional cooperation forums should ensure cooperation amongst themselves and the IMO in order to draw on the different experiences gained;

.5 every country is recommended to ensure that each national RCC, which may be contacted by RCCs from other countries, is capable at all times of communicating in English. Thus, at least one person with a satisfactory knowledge of the English language - both written and spoken - should always be on duty;

.6 in order to minimize coordination problems and possible delays in cases when distress/safety messages related to a specific area are received by Coast Earth Stations and RCCs in other countries, it is recommended to arrange common meetings/seminars for key personnel from both areas for the exchange of views and to establish suitable procedures and actions in different types of situations. Consideration should also be given to arranging common exercises to verify that procedures and actions are effective;

[1] Examples of such agreements include the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP), details of which may be found at www.recaap.org; the Memorandum of Understanding on the Establishment of a Regional Integrated Coast Guard Network in West and Central Africa; and the Code of Conduct concerning the repression of piracy and armed robbery against ships in the Western Indian Ocean and the Gulf of Aden (the Djibouti Code of Conduct).

.7 if an attack is reported in an area covered by NAVTEX transmissions, a piracy/armed robbery attack warning with category "Important" or "Vital", as appropriate, should be transmitted whenever such warnings can be transmitted sufficiently early to enable ships to take precautions appropriate to preventing attacks. If an attack is reported in an area which is not covered by NAVTEX transmissions, a piracy/armed robbery attack warning should be transmitted as an EGC SafetyNET message through the INMARSAT system. In this respect, relevant authorities are recommended to make arrangements with one or more Coast Earth Station(s) covering relevant areas, so as to be registered as "information providers"; and

.8 those countries that have established, or which plan to establish, radar surveillance systems, are recommended to investigate the potential suitability of such facilities for anti-piracy/armed robbery purposes. If such facilities are judged to be suitable for such purposes, the facilities and procedures necessary for their rapid and efficient use should be established.

34 Governments should coordinate with the shipowner or the company and the coastal State when receiving a ship security alert. It is important that any response to an incident is well planned and executed, and emphasizes the safety of the crew. Those involved should be as familiar as possible with a ship environment. Therefore, those responsible for responding to acts of piracy or armed robbery of ships, whether at sea or in port, should be trained in the general layout and features of the types of ship most likely to be encountered. Shipowners should be encouraged to cooperate with the security forces by providing access to their ships for the necessary familiarization.

35 Coastal States should consider the use of suitably equipped helicopters and other suitable means in countering acts of piracy and armed robbery. Security forces should consider the use of modern night vision equipment and other applicable modern technology.

36 A local rule of the road amendment allowing ships under attack to flash or occult their "not under command" lights should be authorized in areas where pirate/armed robbery attacks are more common.

37 States with adjacent coastal waters affected by pirates and armed robbers should develop or maintain coordinated patrols by both ships and aircraft.

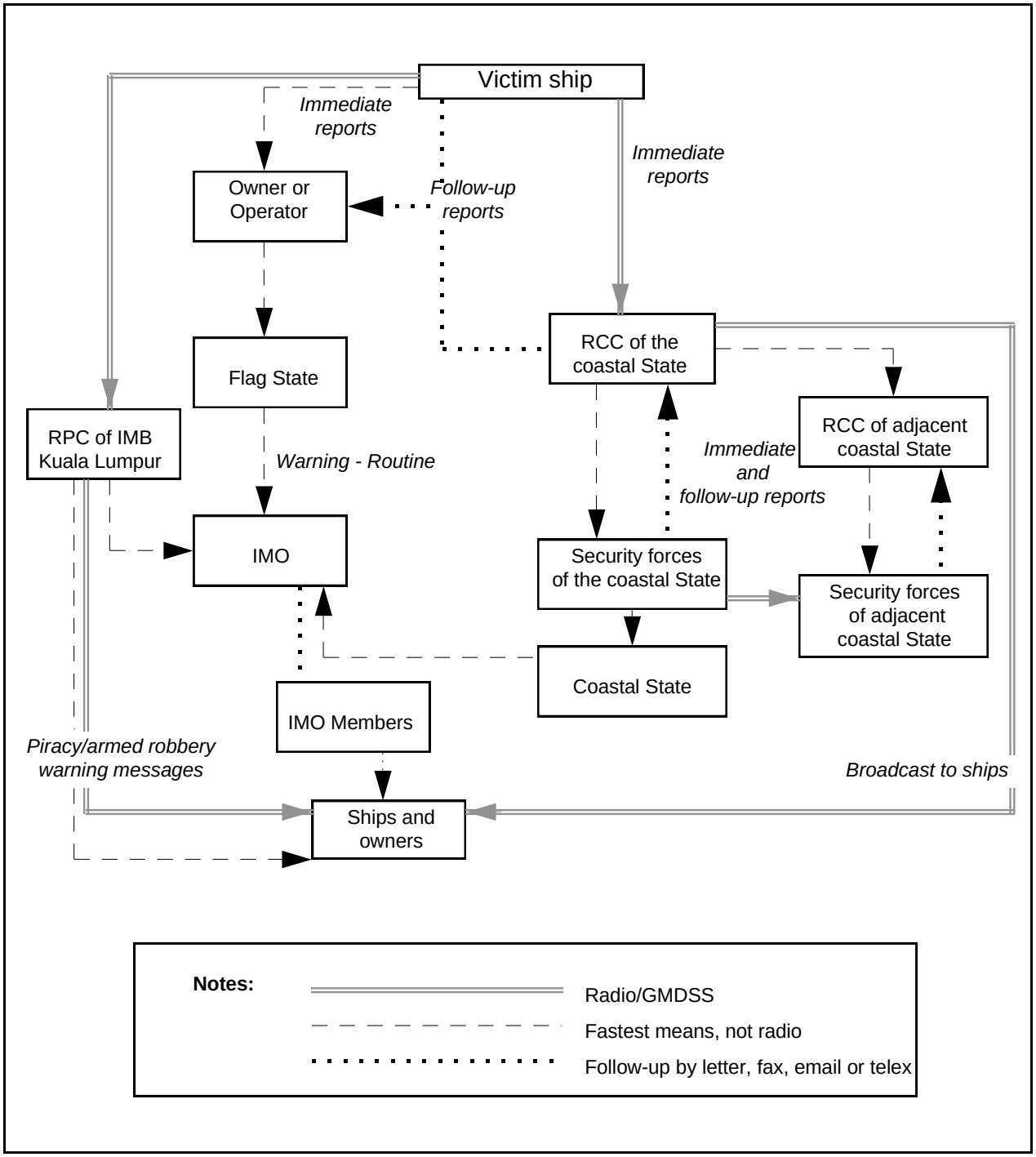
38 Security forces and Governments should maintain close liaison with their counterparts in neighbouring States to facilitate the apprehension and prosecution of criminals involved in such unlawful acts. Some countries have already a well-established coordination which is also used for preventing and suppressing piracy and armed robbery.

39 RCC personnel should be instructed on the most efficient means of communicating reports on piracy and armed robbery, which they receive. Depending on the circumstances, this may require forwarding the reports to another RCC or coast radio station, notifying security forces or patrol craft in the area and taking steps to have a broadcast warning issued or other suitable action taken.

40 RCCs should be encouraged to forward all received reports of piracy and armed robbery to IMO. States are encouraged to share any information with IMB's Piracy Reporting Centre and the ReCAAP Focal Points.

APPENDIX 1

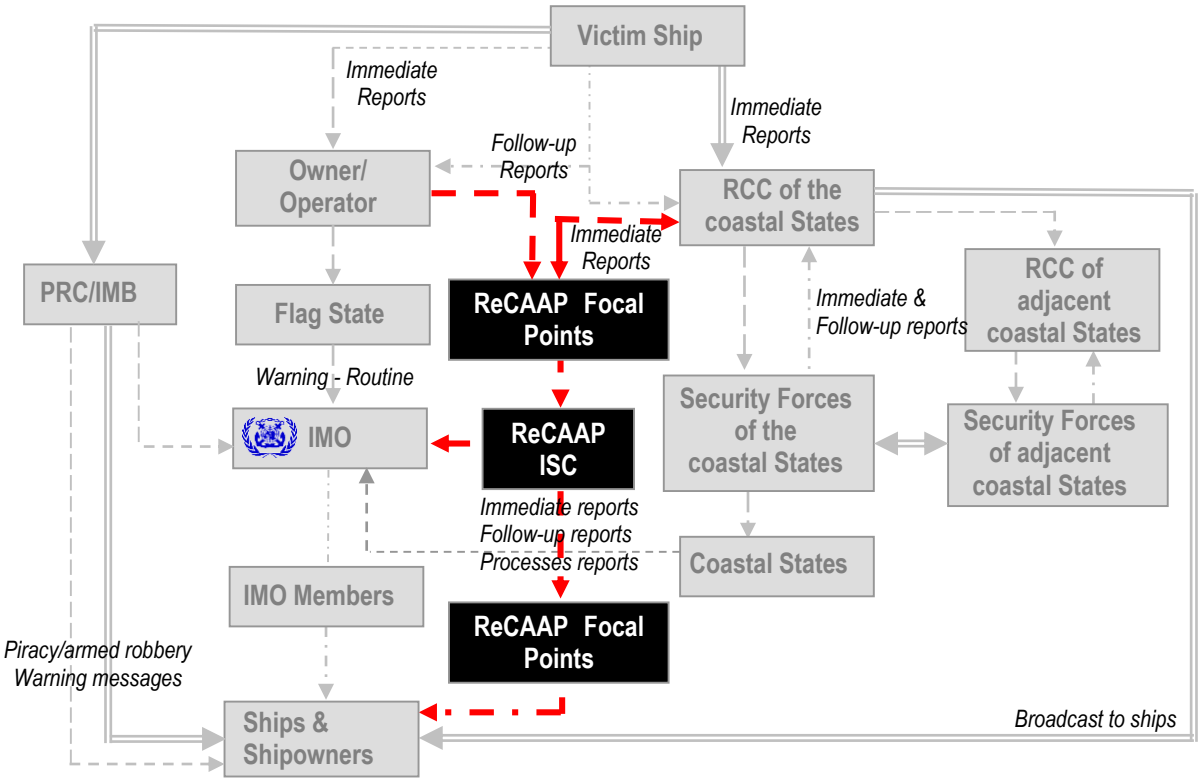
STATISTICS, FLOW DIAGRAMS AND OTHER RELEVANT INFORMATION



Flow diagram for attacks in coastal waters

APPENDIX 2

FLOW DIAGRAM FOR REPORTING INCIDENTS IN ASIA



Legend:

Radio/GMDSS	:
Fastest means	:
Follow-up comms	:

Notes:

1. *In the Asian region, the RCCs of some ReCAAP Contracting Parties are also their ReCAAP Focal Points (FPs). These Focal Points also disseminate incident information internally to their respective RCCs, maritime authorities and law enforcement agencies as appropriate.*
2. *Coastal States (in the context of this addendum) refer only to those who are Contracting Parties to the ReCAAP.*
3. *The incident reporting process in Asia does not change other reporting processes for incidents already in practice.*

APPENDIX 3

"PHASES" RELATED TO VOYAGES IN PIRACY AND ARMED ROBBERY THREAT AREAS

Phase Symbol	Phase Description
A	Approaching a piracy/armed robbery threat area (1 hour prior to entering)
B	Entering a piracy/armed robbery threat area
C	Inside a piracy/armed robbery threat area, but no suspect piracy/armed robbery vessel detected
D	Inside a piracy/armed robbery threat area: suspect piracy/armed robbery vessel detected
E	Certainty that piracy/armed robbery will be attempted
F	Pirate/armed robbery vessel in proximity to, or in contact with, own ship
G	Pirates/armed robbers start attempts to enter ship
H	Pirates/armed robbers have succeeded in entering ship
I	Pirates/armed robbers have one or more of the ship's personnel in their control/custody
J	The pirates/armed robbers have gained access to the bridge or the master's office
K	The pirates/armed robbers have stolen property/money, etc.
L	The pirates/armed robbers start to disembark
M	The pirates/armed robbers have disembarked
N	The pirate/armed robbery vessel is no longer in contact with the ship
O	Own ship leaves the piracy/armed robbery threat area

APPENDIX 4

SHIPS' MESSAGE FORMATS

Report 1 – Initial message – Piracy/armed robbery attack alert

1 Ship's name and, callsign, IMO number, INMARSAT IDs (plus ocean region code) and MMSI

MAYDAY/DISTRESS ALERT (see note)

URGENCY SIGNAL

PIRACY/ARMED ROBBERY ATTACK

2 Ship's position (and time of position UTC)

Latitude Longitude
Course Speed KTS

3 Nature of event

Note: It is expected that this message will be a Distress Message because the ship or persons will be in grave or imminent danger when under attack. Where this is not the case, the word MAYDAY/DISTRESS ALERT is to be omitted.

Use of distress priority (3) in the INMARSAT system will not require MAYDAY/DISTRESS ALERT to be included.

Report 2 – Follow-up report – Piracy/armed robbery attack alert

1 Ship's name and, callsign, IMO number

2 Reference initial PIRACY/ARMED ROBBERY ALERT

3 Position of incident

Latitude Longitude
Name of the area

4 Details of incident, e.g.:

While sailing, at anchor or at berth?
Method of attack
Description/number of suspect craft
Number and brief description of pirates/robbers
What kind of weapons did the pirates/robbers carry?
Any other information (e.g. language spoken)
Injuries to crew and passengers
Damage to ship (Which part of the ship was attacked?)
Brief details of stolen property/cargo
Action taken by the master and crew
Was incident reported to the coastal authority and to whom?
Action taken by the Coastal State

5 Last observed movements of pirate/suspect craft, e.g.:
Date/time/course/position/speed

6 Assistance required

7 Preferred communications with reporting ship, e.g.:

Appropriate Coast Radio Station
HF/MF/VHF
INMARSAT IDs (plus ocean region code)
MMSI

8 Date/time of report (UTC)

APPENDIX 5

FORMAT FOR REPORTING TO IMO THROUGH MARITIME ADMINISTRATIONS OR INTERNATIONAL ORGANIZATIONS

2* Ship's name and IMO number
Type of ship
Flag
Gross tonnage

3 Date and time

4 Latitude Longitude
Name of the area**
While sailing, at anchor or at berth?

5 Method of attack
Description/number of suspect craft
Number and brief description of pirates/robbers
What kind of weapons did the pirates/robbers carry?
Any other information (e.g. language spoken)

6 Injuries to crew and passengers
Damage to ship (Which part of the ship was attacked?)
Brief details of stolen property/cargo

7 Action taken by the master and crew

8 Was incident reported to the coastal authority and to whom?

9 Reporting State or international organization

10 Action taken by the Coastal State

* Corresponding to the column numbers in the annex to the IMO monthly circulars.

** The following definition of piracy is contained in article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS):

"Piracy consists of any of the following acts:

(a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:

(i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;

(ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;

(b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;

(c) any act inciting or of intentionally facilitating an act described in sub-paragraph (a) or (b)."

APPENDIX 6

DRAFT* REGIONAL AGREEMENT ON COOPERATION IN PREVENTING AND SUPPRESSING ACTS OF PIRACY AND ARMED ROBBERY AGAINST SHIPS

Note: Due to different circumstances among States, this example agreement may be varied to meet specific situations.

Agreement between the Governments of _____, _____,

_____,_____, and _____

(Hereinafter, "the Parties");

Bearing in mind the complex nature of the problem of piracy and armed robbery against ships;

Having regard to the urgent need for international cooperation in preventing and suppressing piracy and armed robbery against ships;

Desiring to promote greater cooperation between the parties and thereby enhance their effectiveness in preventing and suppressing piracy and armed robbery against ships;

Being conscious of the fact that, in order to prevent and suppress piracy and armed robbery against ships effectively and efficiently, the active participation of all States affected is needed;

Taking into account that the Governments do not have sufficient technical and material resources to prevent and suppress piracy and armed robbery against ships independently;

Recognizing that piracy and armed robbery are international and transnational threats to seafarers, property and the environment; and conscious of the fact that the Parties are experiencing increased incidents of piracy and armed robbery within their maritime zones and adjoining international waters;

Have agreed as follows:

Definitions

For the purpose of this Agreement, unless expressly provided otherwise:

1 "Piracy" means those acts as defined in Article 101 of the United Nations Convention on the Law of the Sea (UNCLOS), 1982.

2 "Armed robbery against ships" means [...].

3 "National waters [and airspace]" means the territorial sea and internal waters of the Parties [and the air space over those States].

* The present draft includes text in square brackets which was left to the discretion of the individual Governments.
Note: attention should also be given to existing regional agreements such as the Djibouti Code of Conduct, the ReCAAP, and the IMO/MOWCA Memorandum of Understanding on the Establishment of a Regional Integrated Coast Guard Network in West and Central Africa.

4 "Law enforcement vessels" mean ships of the Parties clearly marked and identifiable as being on government non-commercial service and authorized to that effect, including any boat and aircraft embarked on such ships, aboard which law enforcement officials are embarked.

[5 "Law enforcement aircraft" means aircraft of the Parties engaged in law enforcement operations or operations in support of law enforcement activities clearly marked and identifiable as being on non-commercial government service and authorized to that effect.]

5[6] "Liaison officer" means one or more law enforcement officials, including boarding teams, of one Party authorized to embark on a law enforcement vessel of another Party.

6[7] "Suspect vessel" means a vessel used for commercial or private purposes in respect of which there are reasonable grounds to suspect it is involved in piracy or armed robbery against ships.

7[8] "Incident Command System" means a regional system for operational/tactical response to acts of piracy and armed robbery against ships providing common terminology, modular organization, integrated communications, unified command structure, consolidated action plans, manageable span of control, designated incident facilities and comprehensive resource management.

Nature and scope of the Agreement

1 The Parties shall cooperate in preventing and suppressing piracy and armed robbery at sea to the fullest extent possible, consistent with available law enforcement resources and related priorities.

2 The Parties undertake to agree on procedures for improving intelligence sharing.

Operations in [and over] national waters

Operations to suppress piracy and armed robbery in the national waters of a Party are subject to the authority of that Party.

Programme for law enforcement officials aboard another Party's vessels

1 The Parties shall establish a law enforcement liaison officer programme among their law enforcement authorities. Each Party may designate a coordinator to organize its programme activities and to notify the other Parties of the types of vessels and officials involved in the programme.

2 The Parties may designate qualified law enforcement officials to act as law enforcement liaison officers.

3 Subject to the law of the Parties involved, these liaison officers may, in appropriate circumstances:

.1 embark on the law enforcement vessels of other Parties;

.2 authorize the pursuit, by the law enforcement vessels on which they are embarked, of suspect vessels fleeing into the territorial waters of the liaison officer's Party;

.3 authorize the law enforcement vessels on which they are embarked to conduct patrols to suppress acts of armed robbery against ships in the liaison officer's Party's national waters; and

.4 enforce the laws of the Parties in national waters, or seaward there from in the exercise of the right of hot pursuit or otherwise in accordance with international law.

4 When a liaison officer is embarked on another Party's vessel, and the enforcement action being carried out is pursuant to the liaison officer's authority, any search or seizure of property, any detention of a person, and any use of force pursuant to this Agreement, whether or not involving weapons, shall be carried out by the liaison officer, except as follows:

.1 crew members of the other Party's vessel may assist in any such action if expressly requested to do so by the liaison officer and only to the extent and in the manner requested. Such request may only be made, agreed to, and acted upon in accordance with the applicable laws and policies; and

.2 such crew members may use force in self-defence, in accordance with the applicable laws and policies.

5 Parties may only conduct operations to suppress piracy and armed robbery in the waters of another Party with the permission of that Party in any of the following circumstances:

.1 an embarked liaison officer so authorizes;

.2 on those exceptional occasions when a suspect vessel, detected seaward of national waters, enters the national waters of another Party and no liaison officer is embarked in a law enforcement vessel, and no law enforcement vessel from the Party whose national waters have been entered by a suspect vessel is immediately available to investigate, the law enforcement vessel may follow the suspect vessel into national waters, in order to board the suspect vessel and secure the scene, while awaiting expeditious instructions and the arrival from law enforcement authorities of the Party in whose national waters the event took place;

.3 on those equally exceptional occasions when a suspect vessel is detected within a Party's national waters, and no liaison officer is embarked from that Party and no law enforcement vessel is immediately available to investigate from that Party, the law enforcement vessel from another Party may enter the national waters, in order to board the suspect vessel and secure the scene, while awaiting expeditious instructions from the law enforcement authorities and the arrival of law enforcement officials of the Party in whose national waters the event has occurred; and

.4 Parties shall provide prior notice to the law enforcement authority of the Party in whose national waters the event took place of action to be taken under subparagraphs .2 and .3 of this paragraph, unless it is not operationally feasible to do so. In any case, notice of the action shall be provided to the relevant law enforcement authority without delay.

[6 When aircraft of the Parties (hereafter referred to as "aircraft") are operating to suppress piracy and armed robbery against ships or supporting such operations, other Parties shall permit those aircraft:

.1 to overfly the territory and waters of other Parties with due regard for the laws and regulations of those Parties for the flight and manoeuvre of aircraft, subject to paragraph 7 of this section; and

.2 to land and remain in national airports, after receiving authorization from the minister of public security, on the occasions and for the time necessary for the proper conduct of operations deemed necessary under this Agreement.

7 The Parties shall, in the interest of flight safety, observe the following procedures for facilitating flights within the national airspace by law enforcement aircraft:

.1 in the event of planned law enforcement operations, Parties shall provide reasonable notice and communication frequencies to the appropriate aviation authorities responsible for air traffic control of planned flights by its aircraft over national territory or waters;

.2 in the event of unplanned operations, the Parties shall exchange information concerning the appropriate communication frequencies and other information pertinent to flight safety; and

.3 any aircraft engaged in law enforcement operations or operations in support of law enforcement activities in accordance with this agreement shall comply with such air navigation and flight safety directions as may be required by pertinent aviation authorities, and with any written operating procedures developed for flight operations within their airspace under this Agreement.]

Operations seaward of the territorial sea

1 Whenever law enforcement officials of a Party encounter a suspect vessel flying the flag of another Party or claiming to be registered in the country of another Party, located seaward of any State's territorial sea, this Agreement constitutes the authorization of that Party for the boarding and search of the suspect vessel and the persons found on board by such officials. If evidence of piracy or armed robbery against ships is found, law enforcement officials may detain the vessel and persons on board pending expeditious disposition instructions from the Government of the flag State.

2 Except as expressly provided herein, this Agreement does not apply to or limit boardings of vessels seaward of any State's territorial sea, conducted by either Party in accordance with international law, whether based, inter alia, on the right of visit, the rendering of assistance to persons, ships, and property in distress or peril, the consent of the shipmaster, or an authorization from the flag State to take law enforcement action.

Jurisdiction over detained vessel

1 In all cases arising in national waters, or concerning vessels flying the flag of a Party seaward of any State's territorial sea, the Party whose flag is being flown by the suspect vessel shall have the primary right to exercise jurisdiction over a detained vessel, cargo and/or persons on board (including seizure, forfeiture, arrest, and prosecution), provided, however, that the Party may, subject to its constitution and laws, waive its primary right to exercise jurisdiction and authorize the enforcement of another Party's law against the vessel, cargo and/or persons on board.

2 Instructions as to the exercise of jurisdiction pursuant to paragraph 1 shall be given without delay.

Implementation

1 Operations to suppress piracy and armed robbery pursuant to this Agreement shall be carried out only against suspect vessels, including vessels without nationality, and vessels assimilated to vessels without nationality.

2 All Parties shall utilize the Incident Command System when operating in conjunction with another Party in an operation within the scope of this Agreement.

3 All Parties undertake to agree on uniform reporting criteria in order to ensure that an accurate assessment of the threat is developed. Furthermore, all Parties shall endeavour to ensure that reporting ships are not unduly detained for investigative purposes. A summary of reports to each Party shall be shared at least annually with the other Parties.

4 A Party conducting a boarding and search pursuant to this Agreement shall promptly notify the flag State of the results thereof. The relevant Party shall timely report to the other Party, consistent with its laws, on the status of all investigations, prosecutions and judicial proceedings resulting from enforcement action taken pursuant to this Agreement where evidence of piracy and armed robbery has been found.

5 Each Party shall ensure that its law enforcement officials, when conducting boardings and searches [and air interception] activities pursuant to this Agreement, act in accordance with the applicable national laws and policies of that Party and with the applicable international law and accepted international practices.

6 Boardings and searches pursuant to this Agreement shall be carried out by law enforcement officials from law enforcement vessels [or aircraft]. The boarding and search teams may operate from such ships [and aircraft] of the relevant Parties, and seaward of the territorial sea of any State, from such ships of other Parties as may be agreed upon by the Parties. The boarding and search team may carry standard law enforcement small arms.

[7 While conducting air intercept activities pursuant to this Agreement, the Parties shall not endanger the lives of persons on board and the safety of civil aircraft.]

7[8] All use of force pursuant to this Agreement shall be in strict accordance with the applicable laws and policies and shall in all cases be the minimum reasonably necessary under the circumstances. Nothing in this Agreement shall impair the exercise of the inherent right of self-defence by law enforcement or other officials of either Party.

8[9] When carrying out operations pursuant to this Agreement, the Parties shall take due account of the possible advantage of conducting boarding and search operations in safer conditions at the closest port of a Party to minimize any prejudice to the legitimate commercial activities of the suspect vessel, or its flag State or any other interested State; the need not to delay unduly the suspect vessel; the need not to endanger the safety of life at sea without endangering the safety of the law enforcement officials or their vessels [or aircraft]; and the need not to endanger the security of the suspect vessel or its cargo.

9[10] To facilitate implementation of this Agreement, each Party shall ensure the Parties are fully informed of its respective applicable laws and policies, particularly those pertaining to the use of force. Each Party shall ensure that all of its law enforcement officials are knowledgeable concerning the applicable laws and policies of the other Parties.

10[11] Assets seized in consequence of any operation undertaken in the national waters of a Party pursuant to this Agreement shall be disposed of in accordance with the laws of the Party. Assets seized in consequence of any operation undertaken seaward of the territorial sea of a Party pursuant to this Agreement shall be disposed of in accordance with the laws of

the seizing Party. To the extent permitted by its laws and upon such terms as it deems appropriate, a Party may, in any case, transfer forfeited assets or proceeds of their sale to another Party. Each transfer generally will reflect the contribution of other Parties to facilitating or effecting the forfeiture of such assets or proceeds.

11[12] The law enforcement authority of one Party (the "first Party") may request, and the law enforcement authority of another Party may authorize, law enforcement officials of the other Party to provide technical assistance to law enforcement officials of the first Party in their boarding and investigation of suspect vessels located in the territory or waters of the first Party.

12[13] Any injury to or loss of life of a law enforcement official of a Party shall normally be remedied in accordance with the laws of that Party. Any other claim submitted for damage, injury, death or loss resulting from an operation carried out under this Agreement shall be processed, considered, and if merited, resolved in favour of the claimant by the Party whose officials conducted the operation, in accordance with the domestic law of that Party, and in a manner consistent with international law. If any loss, injury or death is suffered as a result of any action taken by the law enforcement or other officials of one Party in contravention of this Agreement, or any improper or unreasonable action is taken by a Party pursuant thereto, the relevant Parties shall, without prejudice to any other legal rights which may be available, consult at the request of a Party to resolve the matter and decide any questions relating to compensation.

13[14] Disputes arising from the interpretation or implementation of this Agreement shall be settled by mutual agreement of the Parties.

14[15] The Parties agree to consult, on at least an annual basis, to evaluate the implementation of this Agreement and to consider enhancing its effectiveness, including the preparation of amendments to this Agreement that take into account increased operational capacity of the law enforcement authorities and officials. In case a difficulty arises concerning the operation of this Agreement, any Party may request consultations with another Party to resolve the matter.

15[16] Nothing in this Agreement is intended to alter the rights and privileges due any individual in any legal proceeding.

16[17] Nothing in this Agreement shall prejudice the position of any Party with regard to the international law of the sea.

Entry into force and duration

1 [Entry into force]

2 [Denunciation]

3 This Agreement shall continue to apply after termination with respect to any administrative or judicial proceedings arising out of actions taken pursuant to this Agreement during the time that it was in force.

In witness whereof, the undersigned, being duly authorized by their respective Governments, have signed this Agreement.

Done at , this day of

INTERNATIONAL MARITIME ORGANIZATION
4 ALBERT EMBANKMENT
LONDON SE1 7SR

Telephone: 020 7735 7611
Fax: 020 7587 3210

IMO

E

Ref. T2-mss/2.11.4.1

MSC.1/Circ.1334
23 June 2009

PIRACY AND ARMED ROBBERY AGAINST SHIPS

Guidance to shipowners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships

1 The Maritime Safety Committee, at its eighty-sixth session (27 May to 5 June 2009), approved a revised MSC/Circ.623/Rev.3 (Guidance to shipowners and ship operators, shipmasters and crews for preventing and suppressing acts of piracy and armed robbery against ships) as given at annex.

2 The revision was carried out on the basis of the outcome of the comprehensive review of the guidance provided by the Organization for preventing and suppressing piracy and armed robbery against ships; and took into account the work of the correspondence group on the review and updating of MSC/Circ.622/Rev.1, MSC/Circ.623/Rev.3 and resolution A.922(22), established by MSC 84.

3 Member Governments and organizations in consultative status with IMO are recommended to bring this circular to the attention of shipowners, ship operators, shipping companies, shipmasters and crews and all other parties concerned.

4 This circular revokes MSC/Circ.623/Rev.3.

***

ANNEX

GUIDANCE TO SHIPOWNERS, COMPANIES[1], SHIP OPERATORS, SHIPMASTERS AND CREWS ON PREVENTING AND SUPPRESSING ACTS OF PIRACY[*] AND ARMED ROBBERY[**] AGAINST SHIPS

Introduction

1 This circular aims at bringing to the attention of shipowners, companies, ship operators masters and crews the precautions to be taken to reduce the risks of piracy on the high seas and armed robbery against ships at anchor, off ports or when underway through a coastal State's territorial waters. It outlines steps that should be taken to reduce the risk of such attacks, possible responses to them and the vital need to report attacks, both successful and unsuccessful, to the authorities of the relevant coastal State and to the ships' own maritime Administration. Such reports are to be made as soon as possible, to enable necessary action to be taken.

2 It is important to bear in mind that shipowners, companies, ship operators, masters and crews can and should take measures to protect themselves and their ships from pirates and armed robbers. While security forces can often advise on these measures, and flag States are required to take such measures as are necessary to ensure that owners and masters accept their responsibility, ultimately it is the responsibility of shipowners, companies, ship operators, masters and ship operators to take seamanlike precautions when their ships navigate in areas where the threat of piracy and armed robbery exists. Planning should give consideration to the crew's welfare during and after a period of captivity by pirates or armed robbers. Before operating in waters where attacks have been known to occur, it is imperative for shipowners, companies, ship operator and masters concerned to gather accurate information on the situation in the area. To this end the information on attacks and attempted attacks gathered, analysed and distributed by the IMO, IMB's Piracy Reporting Centre

---

[1] The term "company" is defined in SOLAS regulations IX/1 and XI-2/1.

[*] The following definition of piracy is contained in Article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS) (article 101):

"Piracy consists of any of the following acts:

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

[**] The Subregional meeting on piracy and armed robbery against ships in the Western Indian Ocean, Gulf of Aden and Red Sea area, held in Dar es Salaam, United Republic of Tanzania, from 14 to 18 April 2008, agreed to modify this definition. Consistent with the ReCAAP Agreement, the "private ends" motive has been added to the definition. The formulation "within internal waters, archipelagic waters and territorial sea" replaced "within a State's jurisdiction". The new formulation reflects the views of France, supported by other States participating in the meeting, that the definition for armed robbery against ships should not be applicable to acts committed seaward of the territorial sea. The new definition reads: "Armed robbery against ships" means any unlawful act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, 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.

and the ReCAAP Information Sharing Centre (ReCAAP ISC)[2], the Maritime Security Centre, Horn of Africa, Governments and others is vital information, upon which precautionary measures should be based.

3 These recommendations have been culled from a number of sources. Where conflicting advice has been apparent, the reason for choosing the recommended course has been stated.

The pirates'/robbers' objective

4 In addition to the hijacking of ships and the holding of the crew hostage, and the theft of cargo, other targets of the attackers include cash in the ship's safe, crew possessions and any portable ship's equipment. When there has been evidence of tampering with containers, it may be an indication that the raiders may initially have gained access when the ship was berthed in port and then gone over the side, with what they could carry. The application of the ISPS Code is an important precautionary measure and a thorough checking of ships' compartments and securing them before leaving ports is therefore strongly encouraged.

Reducing the temptation for piracy and armed robbery

Cash in the ship's safe

5 The belief that large sums of cash are carried in the master's safe attracts attackers. In some cases this belief has been justified and sums have been stolen. While carrying cash may sometimes be necessary to meet operational needs and crew requirements and to overcome exchange control restrictions in some States, it acts as a magnet for attackers and they will intimidate and take hostage the master or crew members until the locations have been revealed. Shipowners should consider ways of eliminating the need to carry large sums of cash on board a ship. When this need arises because of exchange control restrictions imposed by States, the matter should be referred to the ship's maritime Administration to consider if representations should be made to encourage a more flexible approach as part of the international response to eliminate attacks by pirates and armed robbers.

Discretion by masters and members of the crew

6 Masters should bear in mind the possibility that attackers are monitoring ship-to-shore communications and using intercepted information to select their targets. Masters should however also be aware that switching off AIS in high-risk areas reduces ability of the supporting naval vessels to track and trace vessels which may require assistance. Caution should also be exercised when transmitting information on cargo or valuables on board by radio in areas where attacks occur.

7 It is up to the master's professional judgement to decide whether the AIS system should be switched off, in order for the ship not to be detected, when entering areas where piracy is an imminent threat, however the master should balance the risk of attack against the need to maintain the safety of navigation and, in particular, the requirements of COLREG Rule 7 on Risk of collision, and should act in accordance with the guidance in resolutions A.917(22) and A.956(23). The master should also be aware that other ships operating in high-risk areas may have taken a decision to

[2] The Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) is a Government-to-Government Agreement that addresses the incidence of piracy and armed robbery against ships in Asia. The status of ReCAAP ISC is an IGO. Further details may be found at www.recaap.org.

switch off the AIS system. In the event of an attack, masters should ensure to the extent feasible that AIS is turned on again and transmitting to enable security forces to locate the vessel.

8 Members of the crew going ashore in ports in affected areas should be advised not to discuss the voyage or cargo particulars with persons unconnected with the ship's business.

Smaller crews

9 The smaller crew numbers now found on board ships also favour the attacker. A small crew engaged in ensuring the safe navigation of their ship through congested or confined waters will have the additional onerous task of maintaining high levels of security surveillance for prolonged periods. Shipowners may wish to consider enhancing security watches if their ship is in waters or at anchor off ports, where attacks occur. Shipowners may wish to consider providing appropriate surveillance and detection equipment to aid their crews and protect their ships.

Recommended practices

10 The recommended practices outlined below are based on reports of incidents, advice published by commercial organizations and measures developed to enhance ship security. The extent to which the recommendations are followed or applied are matters solely for the owners or masters of ships operating in areas where attacks occur. The shipping industry would also benefit from consulting other existing recommendations, including those given by the ReCAAP ISC[3], the IMB Piracy Reporting Centre, BIMCO, ICS and other industry bodies.

11 Given that the masters are often required to follow multiple reporting procedures in these difficult circumstances, it is necessary to simplify these procedures as far as operationally feasible. It is therefore recommended that in the event of an occurrence masters should report all actual or attempted attacks of piracy and armed robbery or threats thereof, to:

(i) the nearest RCC or regional piracy focal point where applicable (e.g., ReCAAP ISC in the Asian region[4]),
(ii) the flag State, and
(iii) the IMB Piracy Reporting Centre[5].

12 The recommended actions are defined as phases related to any voyage in a piracy and armed robbery threat area. The phases define the main stages in all situations of pre-piracy or armed robbery, attempted piracy or armed robbery and confirmed piracy or armed robbery. Depending on the development of any one situation, they may or may not materialize. A list of phases is given in Appendix 3.

---

3 The ReCAAP ISC collates and analyses information concerning piracy and armed robbery against ships, and publishes regular reports which identify patterns and trends, highlight good practices and recommend preventive measures.

4 See Appendices 1 and 2 to this circular regarding the information-sharing and incident-reporting processes generally and in the Asian region.

5 The IMB Piracy Reporting Centre is manned 24 hours a day and set up to receive and promulgate reports of attacks or attempted attacks worldwide.

The pre-piracy/armed robbery phase

13 Written procedures on how to prevent or suppress attacks of pirates and armed robbers should be found either in the ship's Safety Management System or in the ship security plan.

14 The entry into force of the ISPS Code and the ISM Code have made security assessments and risk assessments an integral part of the safety and security precautions. Measures to prevent and suppress piracy and armed robbery against ships should be part of either the emergency response procedures in the safety management system, or as a situation that requires increased alertness, should become a part of the procedures in the ship security plan.

15 All ships operating in waters or ports where attacks occur should carry out a security assessment as a preparation for development of measures to prevent attacks of pirates or armed robbers against ships and on how to react should an attack occur. This should be included as a part of the emergency response procedures in the safety management system or a part of the procedures in the ship security plan. The security assessment should take into account the basic parameters of the operation including:

.1 the risks that may be faced including any information given on characteristics of piracy or armed robbery in the specific area;

.2 the ship's actual size, freeboard, maximum speed, and the type of cargo;

.3 the number of crew members available, their proficiency and training;

.4 the ability to establish secure areas on board ship; and

.5 the equipment on board, including any surveillance and detection equipment that has been provided.

16 The ship security plan* or emergency response procedures should be prepared based on the risk assessment, detailing predetermined responses to address increases and decreases in threat levels.

The measures should, *inter alia*, cover:

.1 the need for enhanced surveillance and the use of lighting, surveillance and detection equipment;

.2 controlling of access to the ship and the restricted areas on the ships by ships' personnel, passengers, visitors, etc.;

.3 prevention of unauthorized intrusion by active and passive devices and measures, such as netting, wire, electric fencing, long-range acoustic devices, as well as the use, when appropriate, of security personnel on vessels transiting high-risk areas, and taking other measures to make it more difficult for pirates to board vessels. The safety of onboard personnel should always be taken into account when installing passive devices on board and awareness information should be provided;

* Guidance can be found in the ISPS Code.

.4 monitoring the security of the ship;

.5 crew responses, if a potential attack is detected or an attack is underway;

.6 the radio alarm procedures to be followed; and

.7 the reports to be made after an attack or an **attempted attack**.

Ship security plans or emergency response procedures should ensure that masters and crews are made fully aware of the risks involved during attacks by pirates or armed robbers. In particular, they should address the dangers that may arise if a crew adopts an aggressive response to an attack. Early detection of a possible attack may often be the **most effective deterrent**. Aggressive responses, once an attack is underway and, in particular, once the attackers have boarded the ship, could significantly increase the risk to the ship and those on board.

17 In accordance with the ship security plan, all doors allowing access to the bridge, engine-room, steering gear compartments, officers' cabins and crew accommodation should be secured and controlled in affected areas and should be regularly inspected. The use of surveillance equipment to monitor the areas as well as regular patrolling can be of merit. The intention should be to establish secure areas which attackers will find difficult to penetrate. Securing by locking or other means of controlling access to unattended spaces adjoining areas could also prove useful.

18 The shipowner, company, operator and master should bear in mind, the seafarer's need for shore leave and access to shore-based welfare facilities and medical care.

19 It is important that any response to an incident is well planned and executed, and those involved should be as familiar as possible with a ship environment. Therefore, those responsible within the security forces for responding to acts of piracy and armed robbery against ships, whether at sea or in port, should be trained in the general layout and features of the types of ships most likely to be encountered and shipowners in consultation with the flag State should cooperate with the security forces in providing access to their ships to allow the necessary onboard familiarization.

Routeing and delaying anchoring

20 If at all possible, ships should be routed away from areas where attacks are known to have taken place and, in particular, seek to avoid bottlenecks. When deciding on a ship's route the company should take into consideration the type of ship, the size and maximum speed as well as the freeboard and the dangerous nature of the cargo. If convoys are offered such a measure should also be considered to avoid serious attacks on ships at sea. If ships are approaching ports where attacks have taken place on ships at anchor, rather than ships underway, and it is known that the ship will have to anchor off port for some time, consideration should be given to delaying anchoring by longer routeing to remain well off shore or other methods by which the period during which the ship will be at risk is reduced. Contact with port authorities should ensure that berthing priorities are not affected. Charter party agreements should recognize that ships may need to delay arrival at ports where attacks occur either when no berth is available for the ship or offshore loading or unloading will be delayed for a protracted period.

Practise the implementation of the ship security plan

21 Prior to entering an area, where attacks have occurred, the ship's crew should have practised the procedures set down in the ship security plan. Alarm signals and procedures should have been thoroughly practised and training and drills carried out. If instructions are to be given over the ship's address systems or personal radios, they must be clearly understood by those who may not have fully mastered the language in which the instructions will be given.

22 In order to ensure higher vigilance upon entering the area where attacks occur, additional specific security briefings should be given to all ship personnel on the threats of piracy, re-emphasizing the procedures for reporting suspicious persons, objects or activities. Full or partial searches of the ship should be carried out regularly while in the area with heightened threat of attack.

23 It cannot be emphasized enough that all possible access points to the ship and any key and secure areas on it must be secured or controlled in port, at anchor and when underway in affected areas. Crews should be trained in the use of any additional surveillance or detection equipment installed on the ship. Planning and training must be on the basis that an attack will take place and not in the belief that with some luck it will not happen. Indications to attackers that the ship has an alert and trained crew implementing a ship security plan will help to deter them from attacking the ship.

Precautions at anchor or in port

24 In areas where attacks occur, the ships' masters should exercise vigilance when their ships are preparing to anchor or while at anchor. Furthermore, it is important to limit, record and control those who are allowed access to a ship when in port or at anchor. Photographing those who board the ship can be a useful deterrent or assist the identification of attackers who may have had access to the ship prior to their attack. Given that attackers may use knowledge of cargo manifests to select their targets, every effort should be made to limit the circulation of documents which give information on the cargoes on board or their location on the ship. Similar precautions should be taken in regard to the circulation of information on crew members' personal valuables and ship's equipment, as these items are also targeted by attackers.

25 Prior to leaving port, the ship should be thoroughly searched and all doors or access points secured or controlled. This is particularly important in the case of the bridge, engine-room, steering space and other vulnerable areas. Doors and access points should be regularly checked thereafter. The means of controlling doors or access points which would need to be used in the event of an emergency on board will need careful consideration. Ship or crew safety should not be compromised. Searches on board for intruders should be conducted in such a way that the safety of the crew performing these duties is not compromised.

26 Security guards employed in port or at anchorage on different ships should be in communication with each other and the port authorities during their watch. The responsibility for vetting such guards lies with the security personnel companies, which themselves should be vetted by the appropriate authorities.

Watchkeeping and vigilance

27 Maintaining vigilance is essential. All too often the first indication of an attack has been when the attackers appear on the bridge or in the master's cabin. Advance warning of a possible

attack will give the opportunity to sound alarms, alert other ships and the coastal authorities, illuminate the suspect craft, undertake evasive manoeuvring or initiate other response procedures. Signs that the ship is aware it is being approached can deter attackers.

28 When ships are in, or approaching areas of known risk of piracy or armed robbery, bridge watches and look-outs should be augmented, bearing in mind that many attacks are mounted from astern. Additional watches on the stern or covering radar "blind spots" should be considered. Companies should consider investing in low-light binoculars for bridge staff and look-outs. Radar should be constantly manned but it may be difficult to detect low profile fast moving craft on ship's radars. A yacht radar mounted on the stern may provide additional radar cover capable of detecting small craft approaching from astern when the ship is underway. Use of an appropriately positioned yacht radar when the ship is at anchor may also provide warning of the close approach of small craft.

29 It is particularly important to maintain a radar and visual watch for craft which may be trailing the ship when underway but which could close in quickly when mounting an attack. Small craft which appear to be matching the speed of the ship on a parallel or following course should always be treated with suspicion. When a suspect craft has been noticed, it is important that an effective all-round watch is maintained for fear the first craft is a decoy with the intention to board the ship from a second craft while attention is focused on the first.

30 In addition to the use of overt means of transmitting alerts, the ship security alert system could be used in the event of a piracy or armed robbery attack. It should, however, be borne in mind that certain non-disclosure issues prevail with regards to the configuration and locations of the system.

31 Companies owning or operating ships that frequently visit areas where attacks occur should consider the purchase and use of more sophisticated visual and electronic devices in order to augment both radar and visual watch capability against attackers' craft at night, thereby improving the prospects of obtaining an early warning of a possible attack. In particular, the provision of night vision devices, small radars to cover the blind stern arcs, closed circuit television and physical devices, such as barbed wire, may be considered. In certain circumstances non-lethal weapons such as acoustic devices, may also be appropriate. Infrared detection and alerting equipment may also be utilized.

Communications procedures

32 The master should ensure that an authorized person responsible for communications is on duty at all time when the ship is in, or approaching, areas where attacks occur. It should be ensured that ship-shore communication methods are tested and report intervals agreed prior to entering the high-risk area. The frequency of reporting should be maintained.

33 Shipowners should report attacks and attempted attacks to any national, regional or subregional reporting systems made available by Governments, including those run by security forces.

34 Where possible, ships raising alerts should specify that an act of "piracy/armed robbery" is in progress, in line with other distress categories such as "sinking" or "on fire". This could have a potential to improve the alerting process and speed of response.

35 Prior to entering areas where attacks have occurred and where the GMDSS installation on board does not have facility for automatically updating the "ship position" data from an associated electronic navigation aid, it is strongly recommended to enter the ship's position at regular intervals into the appropriate communications equipment manually. It is recommended that owners initiate the GMDSS INMARSAT "C" alarm programme before entering affected areas for use when appropriate.

36 When entering waters where piracy or armed robbery activities have been reported – especially if the AIS is turned off for security reasons – the ship should routinely transmit its position to the shipping company at given intervals, thereby giving the shipping company a first notice that something is amiss if the transmissions are interrupted. Masters should act in accordance with the guidance in resolution A.917(22) on Guidelines for the onboard operational use of shipborne automatic identification systems (AIS) and resolution A.956(23) on Amendments to the guidelines for the onboard operational use of shipborne automatic identification systems (AIS) (resolution A.917(22)) concerning the turning off of AIS. In the event of an attack, masters should ensure to the extent feasible that AIS is turned on and transmitting to enable security forces to locate the vessel.

Radio watchkeeping and responses

37 A constant radio watch should be maintained with the appropriate shore or naval authorities when in areas where attacks have occurred. Continuous watch should also be maintained on all distress and safety frequencies channels or frequencies which could have been determined by local authorities for certain areas. Ships should also ensure all maritime safety information broadcasts for the area monitored. As it is anticipated that INMARSAT's enhanced group calling system (EGC) will normally be used for such broadcasts using the SafetyNET service, owners should ensure a suitably configured EGC receiver is continuously available when in, or approaching areas where there is risk of attack. Owners should also consider fitting a dedicated receiver for this purpose, i.e. one that is not incorporated into a Ship Earth Station used for commercial purposes to ensure no urgent broadcasts are missed.

38 IMO recommends in MSC.1/Circ.1333 that Governments should arrange for RCCs to be able to pass reports of attacks to the appropriate security forces. As for the reports from the ship, see paragraphs 11, and 39 to 44, below.

39 If suspicious movements are identified which may result in an imminent attack, the ship is advised to contact the relevant RCC, the flag State or other relevant information centres such as the IMB Piracy Reporting Centre or the ReCAAP ISC. Where the master believes these movements could constitute a direct danger to navigation, consideration should be given to broadcasting an "All stations (CQ)" "danger message" as a warning to other ships in the vicinity as well as advising the appropriate RCC. A danger message should be transmitted in plain language using the "safety" priority. All such measures shall be preceded by the safety signal (Sécurité)[6].

40 When, in his/her opinion, there is conclusive evidence that the safety of the ship is threatened, the master should immediately contact the relevant RCC or, in certain areas, with the radio stations which could have been recommended by local authorities, and if considered appropriate, authorize broadcast of an "All Stations" "Urgent Message" any radiocommunications

[6] Specific guidance in respect of waters off the coast of Somalia has been issued as MSC.1/Circ.1332 and also MSC.1/Circ.1302.

service he/she considers appropriate or which could have been recommended by local authorities, e.g., INMARSAT, etc. All such messages shall be preceded by the appropriate Urgency signal (PAN PAN) and/or a DSC call using the "all ships urgency" category. If the Urgency signal has been used and an attack does not, in fact, develop, the ship should cancel the message as soon as it knows that action is no longer necessary. This message of cancellation should likewise be addressed to "all stations".

41 Should an attack occur and, in the opinion of the master, the ship or crew are in grave and imminent danger requiring immediate assistance, the master should immediately authorize the broadcasting of a distress message, preceded by the appropriate distress alerts (MAYDAY, DSC, etc.), using all available radiocommunications systems. To minimize delays, if using a ship earth station, ships should ensure the coast earth station associated with the RCC is used. For ships subject to the ISPS Code, a distress signal should also be sent to the flag State using the most expeditious means for example the ships security alert system. All ships should however report the attack to the flag State to help the investigation of incidents involving ships entitled to fly their flag.

42 The ship may be able to send a covert piracy alert to an RCC. However, as pirates may be on board the ship and within audible range of the communication equipment, when the RCC sends an acknowledgement of receipt and attempts to establish communication, they could be alerted to the fact that a piracy alert has been transmitted. This knowledge may serve to further endanger the lives of the crew on board the ship. RCCs and others should, therefore, be aware of the danger of unwillingly alerting the pirates that a distress alert or other communication has been transmitted by the ship.

43 Masters should bear in mind that the distress signal is provided for use only in case of **imminent** danger and its use for less urgent purposes might result in insufficient attention being paid to calls from ships really in need of immediate assistance. Care and discretion must be employed in its use, to prevent its devaluation in the future. Where the transmission of the Distress signal is not fully justified, use should be made of the Urgency signal. The Urgency signal has priority over all communications other than distress.

Standard ships' message formats

44 The standard ships' message formats given in Appendix 4 should be used for all piracy/armed robbery initial and follow-up alert reports.

Lighting

45 Ships should use the maximum lighting available consistent with safe navigation, having regard in particular to the provisions of Rule 20(b) of the 1972 Collision Regulations. Bow and overside lights should be left on if it can be done without endangering navigation. Ships must not keep on deck lights when underway, as it may lead other ships to assume the ship is at anchor. Wide beam floods could illuminate the area astern of the ship. Signal projector lights can be used systematically to probe for suspect craft using the radar guidance if possible. So far as is practicable crew members on duty outside the ship's secure areas when in port or at anchor should avail themselves of shadow and avoid being silhouetted by deck lights as this may make them targets for seizure by approaching attackers.

46 Based on specific information on acts of piracy and armed robbery at sea in specific regions, ships may consider travelling blacked out except for mandatory navigation lights. This may prevent attackers establishing points of reference when approaching a ship. In addition, turning on the ship's lights as attackers approach could alert them that they have been seen, dazzle them and encourage them to desist. It is difficult, however, to maintain full blackout on a merchant ship. The effectiveness of this approach will ultimately depend in part on the level of moonlight, but primarily on the vigilance of the ship's crew. While suddenly turning on the ship's light may alarm or dazzle attackers, it could also place the crew at a disadvantage at a crucial point through temporary loss of their night vision.

Secure areas

47 In accordance with the ship security plan, all doors allowing access to the bridge, engine-room, steering gear compartments, officers' cabins and crew accommodation should be secured and controlled at all times and should be regularly inspected. The intention should be to establish secure areas which attackers will find difficult to penetrate. Consideration should be given to the installation of special access control systems to the ship's secure areas. Ports, scuttles and windows which could provide access to such secure areas should be securely closed and should have laminated glass, if possible. Deadlights should be shut and clipped tightly. The internal doors within secure areas which give immediate access to key areas such as the bridge, radio room, engine-room and master's cabin should be strengthened and have special access control systems and automatic alarms.

48 Securing doors providing access to, and egress from, secure or key areas may give rise to concern over safety in the event of an accident. In any situation where there is a conflict between safety and security, the safety requirements should be paramount. Nevertheless, attempts should be made to incorporate appropriate safety provisions while allowing accesses and exits to be secured or controlled.

49 Owners may wish to consider providing closed-circuit television (CCTV) coverage and recording of the main access points to the ship's secure areas, the corridors approaching the entrances to key areas and the bridge. The allocation of additional personnel to guarding and patrolling of restricted areas can be a useful preventive measure.

50 To prevent seizure of individual crew members by attackers – seizure and threatening a crew member is one of the more common means of attackers gaining control over a ship – all crew members not engaged on essential outside duties should remain within a secure area during the hours of darkness. Those whose duties necessarily involve working outside such areas at night should remain in regular communication with the bridge, it may be the first indication of an attack if the watchkeeper does not report in, if manning permits work in pairs, make irregular rounds on the deck and should have practised using alternative routes to return to a secure area in the event of an attack. Crew members who fear they may not be able to return to a secure area during an attack should select places in advance in which they can take temporary refuge.

51 There should be designated muster areas within the ship's secure areas where the crew can muster during an attack and communicate their location and numbers to the bridge.

Alarms

52 Alarm signals, including the ship's whistle, should be sounded on the approach of attackers. Alarms and signs of response can discourage attackers. Alarm signals or announcements which provide an indication at the point at which the attacker may board, or have boarded, may help crew members in exposed locations select the most appropriate route to return to a secure area. Announcements made by the crew should be made in the working language of the ship.

53 The crew initial familiarization checklist should specifically state the various alarms used on board the vessel, the response and muster station to each of these alarms. The alarms and alarm signals should be standardized throughout the fleet and not be specific.

Use of distress flares

54 The only flares authorized for carriage on board ship are intended for use if the ship is in distress and is in need of immediate assistance. As with the unwarranted use of the distress signal on the radio (see paragraph 43 above), use of distress flares simply to alert shipping rather than to indicate that the ship is in grave and imminent danger may reduce their effect in the situations in which they are intended to be used and responded to. Radio transmissions should be used to alert shipping of the risk of attacks rather than distress flares. Distress flares should only be used when the master considers that the attackers' actions are putting his/her ship in imminent danger.

Use of defensive measures

55 Experiences show that robust actions from the ship which is approached by pirates may discourage the attackers. Outrunning attacks may be an appropriate preventive manoeuvre. If the situation permits, the speed should be increased and maintained at the maximum level. Provided that navigational safety allows, masters should also consider "riding off" attackers' craft by heavy wheel movements and turning into wind so as to remove any lee from either side of the ship. Heavy wheel movements should only be used when attackers are alongside and boarding is imminent. The effect of the bow wave and wash may deter would-be attackers and make it difficult for them to attach poles or grappling irons to the ship. Manoeuvres of this kind should not be used in confined or congested waters or close inshore or by ships constrained by their draught in the confined deep water routes found, for example, in the Straits of Malacca and Singapore.

Use of passive and non-lethal devices

56 The use of passive and non-lethal measures such as netting, wire, electric fencing, and long-range acoustic devices may be appropriate preventive measures to deter attackers and delay boarding.

57 The use of water hoses should also be considered though they may be difficult to train if evasive manoeuvring is also taking place. Water pressures of 80 lb per square inch and above have deterred and repulsed attackers. Not only does the attacker have to fight against the jet of water but the flow may swamp his/her boat and damage engines and electrical systems. Special fittings for training hoses could be considered which would also provide protection for the hose operator. A number of spare fire hoses could be rigged and tied down to be pressurized at short notice if a potential attack is detected.

58 Employing evasive manoeuvres and hoses must rest on a determination to successfully deter attackers or to delay their boarding to allow all crew members to gain the sanctuary of secure areas. Continued heavy wheel movements with attackers on board may lessen their confidence that they will be able to return safely to their craft and may persuade them to disembark quickly. However, responses of this kind could lead to reprisals by the attackers if they seize crew members and should not be engaged in unless the master is convinced he can use them to advantage and without risk to those on board. They should not be used if the attackers have already seized crew members.

Firearms

59 With respect to the carriage of firearms on board, masters, shipowners and companies should be aware that ships entering the territorial sea and/or ports of a State are subject to that State's legislation. It should be borne in mind that importation of firearms is subject to port and coastal State regulations. It should also be borne in mind that carrying firearms may pose an even greater danger if the ship is carrying flammable cargo or similar types of dangerous goods.

Non-arming of seafarers

60 The carrying and use of firearms by seafarers for personal protection or for the protection of a ship is strongly discouraged. Seafarers are civilians and the use of firearms requires special training and aptitudes and the risk of accidents with firearms carried on board ship is great. Carriage of arms on board ship may encourage attackers to carry firearms or even more dangerous weapons, thereby escalating an already dangerous situation. Any firearm on board may itself become an attractive target for an attacker.

61 It should also be borne in mind that shooting at suspected pirates may impose a legal risk for the master, shipowner or company, such as collateral damages. In some jurisdictions, killing a national may have unforeseen consequences even for a person who believes he or she has acted in self defence. Also the differing customs or security requirements for the carriage and importation of firearms should be considered, as taking a small handgun into the territory of some countries may be considered an offence.

Use of unarmed security personnel

62 The use of unarmed security personnel is a matter for individual shipowners, companies, and ship operators to decide. The use of unarmed security personnel to provide security advice and an enhanced lookout capability could be considered.

Use of privately contracted armed security personnel

63 If armed security personnel are allowed on board, the master, shipowner, operator and company should take into account the possible escalation of violence and other risks. However, the use of privately contracted armed security personnel on board merchant ships and fishing vessels is a matter for flag State to determine in consultation with shipowners, operators and companies. Masters, shipowners, operators and companies should contact the flag State and seek clarity of the national policy with respect to the carriage of armed security personnel. All legal requirements of flag, port and coastal States should be met.

Military teams or law enforcement officers duly authorized by Government

64 The use of military teams or law enforcement officers duly authorized by the Government of the flag State to carry firearms for the security of merchant ships or fishing vessels is a matter for the flag State to authorize in consultation with shipowners, operators and companies. The carriage of such teams may be required or recommended when the ship is transiting or operating in areas if high risk. Due to rules of engagement defined by their Government, or in coalition with other Governments, boarding conditions should be defined by the States involved, including the flag State. The shipowner, operator and company should always consult the flag State prior to embarking such teams.

The phases of suspected or attempted piracy/armed robbery attack

Suspected piracy/armed robbery vessel detected

65 Early detection of suspected attacks must be the first line of defence. If the vigilance and surveillance has been successful, a pirate/armed robbery vessel will be detected early. This is the stage at which the security forces of the nearest littoral or coastal State must be informed through the RCC, using the ships' message format contained in Appendix 4. The ship's crew should be warned and, if not already in their defensive positions, they should move to them. Appropriate passive and active measures, such as evasive manoeuvres and hoses should be vigorously employed as detailed in the preparation phase or in the ship's security plan.

66 Shipowners, company, ship operator and master should be aware of any UN Security Council, IMO or any other UN resolutions on piracy and armed robbery against ships and any recommendations therein relevant to the shipowner, operator, master and crew when operating in areas where piracy or armed robbery against ships occur.

Being certain that piracy/armed robbery will be attempted

67 If not already in touch with the security forces of the littoral coastal State, efforts should be made to establish contact. Crew preparations should be completed and, where a local rule of the road allows ships under attack to do so, a combination of sound and light signals should be made to warn other ships in the vicinity that an attack is about to take place. Vigorous manoeuvring should be continued and maximum speed should be sustained if navigation conditions permit. Nothing in these guidelines should be read as limiting the master's authority to take action deemed necessary by the master to protect the lives of passengers and crew.

Pirate/armed robbery vessel in proximity to, or in contact with, own ship

68 Vigorous use of hoses in the boarding area should be continued. It may be possible to cast off grappling hooks and poles, provided the ship's crews are not put to unnecessary danger.

69 While giving due consideration to safety of crew, vessel and environment it is recommended that masters should not slow down and stop, as far as practicable, when pursued by or fired upon by pirates/armed robbers intending to board and hijack the vessel. Where the pirates/armed robbers operate from a mother ship, masters should consider steering away from the mother ship thus increasing the distance between the attacking craft and the mother ship.

Pirates/armed robbers start to board ship

70 Timing during this phase will be critical and as soon as it is appreciated that a boarding is inevitable all crew should be ordered to seek their secure positions and activate any systems for raising the alarm including the ship security alert system.

Pirates/armed robbers have succeeded in entering ship

71 Early detection of potential attacks must be the first line of defence, action to prevent the attackers actually boarding the second, but there will be incidents when attackers succeed in boarding a ship. The majority of pirates and armed robbers are opportunists seeking an easy target and time may not be on their side, particularly if the crews are aware they are on board and are raising the alarm. However, the attackers may seek to compensate for the pressure of time they face by escalating their threats or the violence they employ. When attackers are on board the actions of the master and crew should be aimed at:

.1 securing the greatest level of safety for those on board the ship;

.2 seeking to ensure that the crew remain in control of the navigation of the ship; and

.3 securing the earliest possible departure of the attackers from the ship.

72 The options available to the master and crew will depend on the extent to which the attackers have secured control of the ship, e.g., by having gained access to the bridge or engine-room, or by seizing crew members who they can threaten, to force the master or crew to comply with their wishes. However, even if the crew are all safely within secure areas, the master will always have to consider the risk to the ship the attackers could cause outside those areas, e.g., by using firebombs to start fires on a tanker or chemical carrier.

73 If the master is certain that all his/her crew are within secure areas and that the attackers cannot gain access or by their actions outside the secure areas they do not place the entire ship at imminent risk, then he/she may consider undertaking evasive manoeuvres of the type referred to above to encourage the attackers to return to their craft.

74 The possibility of a sortie by a well-organized crew has, in the past, successfully persuaded attackers to leave a ship but the use of this tactic is only appropriate if it can be undertaken at no risk to the crew. For an action like this to be attempted the master must have clear knowledge of where the attackers are on the ship, that they are not carrying firearms or other potentially lethal weapons and that the number of crew involved significantly outnumbers the attackers they will face. If a sortie party can use water hoses, they stand an increased chance of success. The intention should be to encourage the attackers back to their craft. Crew members should not seek to come between the attackers and their craft nor should they seek to capture attackers as to do so may increase the resistance the attackers offer which will, in turn, increase the risk faced by members of the sortie party. Once outside the secure area, the sortie party should always stay together. Pursuit of an individual attacker by a lone crew member may be attractive but if it results in the crew member being isolated and seized by the attackers, the advantage turns to the attackers. Crew members should operate together and remain in constant communication with the bridge and should be recalled if their line of withdrawal to a secure area is threatened.

75 If the crew do apprehend an attacker, he/she should be placed in secure confinement and well cared for. Arrangements should be made to transfer him/her to the custody of officers of the security forces of a coastal State at the earliest possible opportunity. Any evidence relating to these activities should also be handed over to the authorities who take him/her into custody.

The pirates/armed robbers begin to gain control and take one or more of the ship's crew into their custody

76 If the attackers have gained control of the engine-room or bridge, have seized crew members or can pose an imminent threat to the safety of a ship, the master or officer in charge should remain calm and, if possible, seek to negotiate with the attackers with the intention of maintaining the crew's control over the navigation of the ship, the safe return of any hostages they may hold and the early departure of the attackers from the ship. There will be many circumstances when compliance with the attackers' demands will be the only safe alternative and resistance or obstruction of any kind could be both futile and dangerous. An extract from United Nations Guidance on surviving as a hostage is given in Appendix 4.

77 In the event of attackers gaining temporary control of the ship, crew members should, if it is safe and practicable, leave Close Circuit Television (CCTV) records running.

78 As there have been occasions when entire crews have been locked up, consideration should be given to secreting equipment within areas in which the crew could be detained to facilitate their early escape.

79 In the event of hijacking a ship, the shipping company should seek expert advice and assistance from professionals to the effect of the safe return of the crew, as handling these situations have shown to be time-consuming and stressful for all parties involved.

The pirates/armed robbers have stolen property/money, etc.

80 At this stage it is essential that the pirates/armed robbers are assured that they have been given everything they demand and a strong reassurance that nothing has been secreted may persuade the pirates/armed robbers to leave.

The pirates/armed robbers start to disembark from the ship

81 If the crew are in their secure positions, it would be unwise of them to leave this security until it is confirmed that the pirates/armed robbers have left the ship.

The pirates/armed robbers have disembarked from the ship

82 A pre-arranged signal on the ship's siren will alert the crew to the "all clear". The company Security Officer should be informed accordingly.

Action after an attack and reporting incidents

83 Immediately after securing the safety of the ship and crew a post attack report (Follow-up report, as shown in Ships' message formats in Appendix 5) should be made to the relevant RCC and, through them, to the security forces of the coastal State concerned. As well as information on the identity and location of the ship, any injuries to crew members or damage to the ship should be

reported, as should the direction in which the attackers departed together with brief details of their numbers and, if possible, a description of their craft. If the crew have apprehended an attacker, that should also be reported in this report.

84 If an attack has resulted in the death of, or serious injury to, any person on board the ship or serious damage to the ship itself, an immediate report should also be sent to the ship's maritime Administration. In any event a report of an attack is vital if follow-up action is to be taken by the ship's maritime Administration. The shipowner, companies, ship operators, shipmasters and crew should cooperate with the investigators and provide the requested information.

85 Any CCTV or other recording of the incident should be secured. If practicable, areas that have been damaged or rifled should be secured and remain untouched by crew members pending possible forensic examination by the security forces of a coastal State. Crew members who came into contact with the attackers should be asked to prepare an individual report on their experience noting, in particular, any distinguishing features which could help subsequent identification of the attackers. A full inventory, including a description of any personal possessions or equipment taken, with serial numbers when known, should also be prepared.

86 As soon as possible after the incident, a fuller report should be transmitted to the authorities of the coastal State in whose waters the attack occurred or, if on the high seas, to the authorities of the nearest coastal State. Due and serious consideration should be given to complying with any request made by the competent authorities of the coastal State to allow officers of the security forces to board the ship, take statements from crew members and undertake forensic and other investigations. Copies of any CCTV recordings, photographs, etc., should be provided if they are available.

87 Ships should take the necessary precautions, and implement the necessary procedures to ensure rapid reporting of any case of attack or attempted attack to the authorities in the relevant coastal States to enhance the possibility of security forces apprehending the attackers.

88 Any report transmitted to a coastal State should also be transmitted to the ship's maritime Administration at the earliest opportunity. A complete report of the incident, including details of any follow-up action that was taken or difficulties that may have been experienced, should eventually be submitted to the ship's maritime Administration. The report received by maritime Administrations may be used in any diplomatic approaches made by the flag State to the Government of the coastal State in which the incident occurred. This will also provide the basis for the report to IMO.

89 The format required for reports to IMO through maritime Administrations or international organizations is attached at Appendix 6. Indeed, at present the lack of adequate and accurate reporting of attacks is directly affecting the ability to secure governmental and international action. Reports may also contribute to future refining and updating any advice that might be issued to ships.

90 Reports to the RCC, coastal State and the ship's maritime Administration should also be made if an attack has been unsuccessful.

91 Using RCCs, as recommended by IMO in MSC/Circ.1073, will eliminate communication difficulties.

On leaving piracy/armed robbery high-risk/high-probability areas

92 On leaving piracy/armed robbery threat areas, shipmasters should make certain that those spaces that need to be unlocked for safety reasons are unlocked, unrig hoses and revert to normal watchkeeping/lighting. However, though ships may be operating outside high-risk/high-probability areas, ship masters may, at their discretion, have ready their anti-piracy/robbery measures in view that the pirates/robbers may attack outside these areas.

Post-incident follow-up

93 A debriefing should be conducted by the owner/master, SSO and CSO to learn from the attack and identify areas of improvement. The debriefing should be conducted immediately after the incident so that the events are fresh and should involve the entire crew.

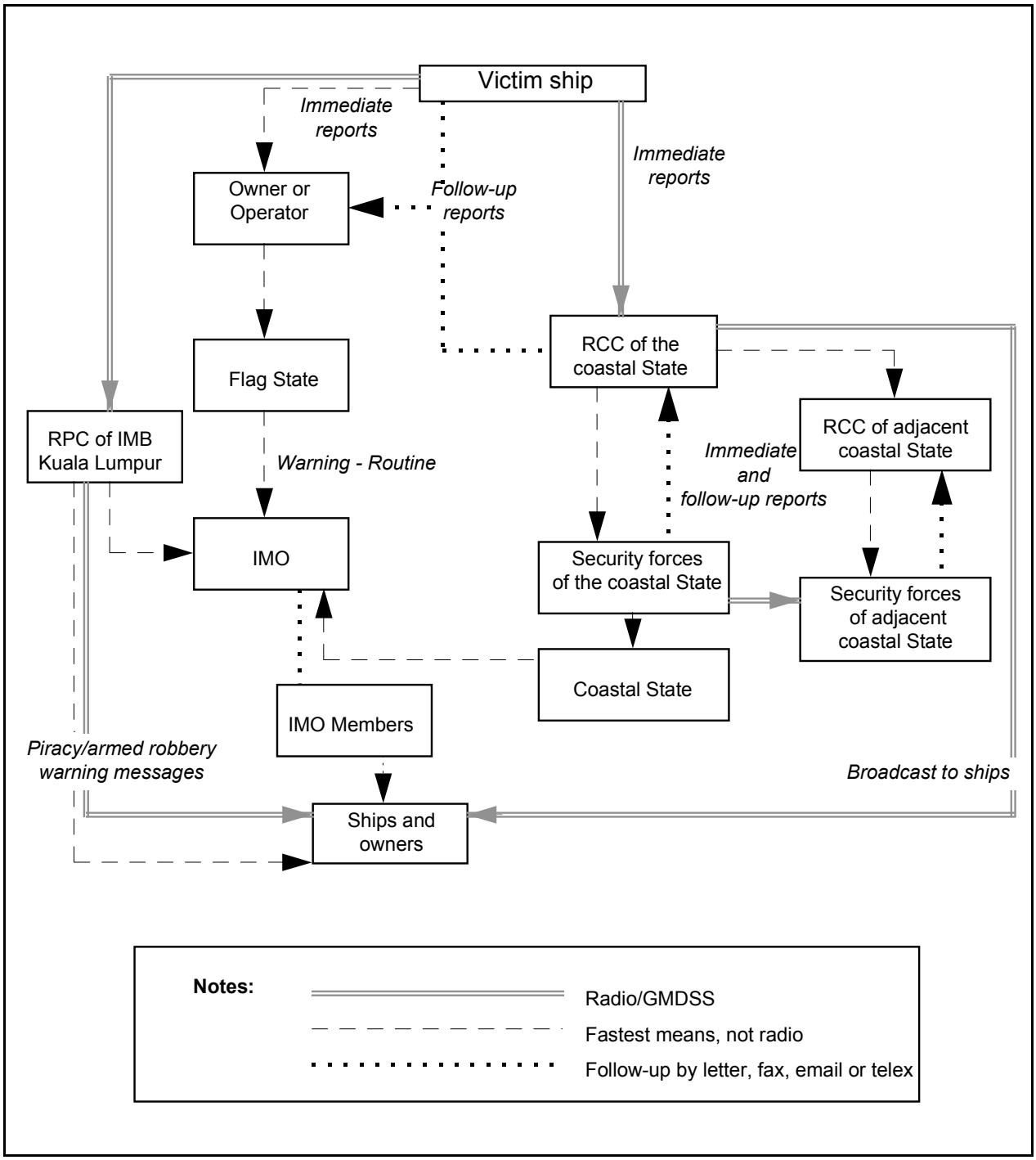
94 The shipowner should be aware that the seafarer may suffer from trauma or similar condition after being victimized under an attack from pirates or armed robbers. The shipowner should offer advice from professionals if the seafarer wishes such assistance. An important first step in reducing the risk from trauma is for masters to debrief crew immediately after the attack or release of a vessel in order to get crew to confront their experiences. An important second step is for counselling professionals to debrief crew as soon as possible after the attack or release of the vessel in order to assist the crew to manage their experiences.

* * *

APPENDIX 1

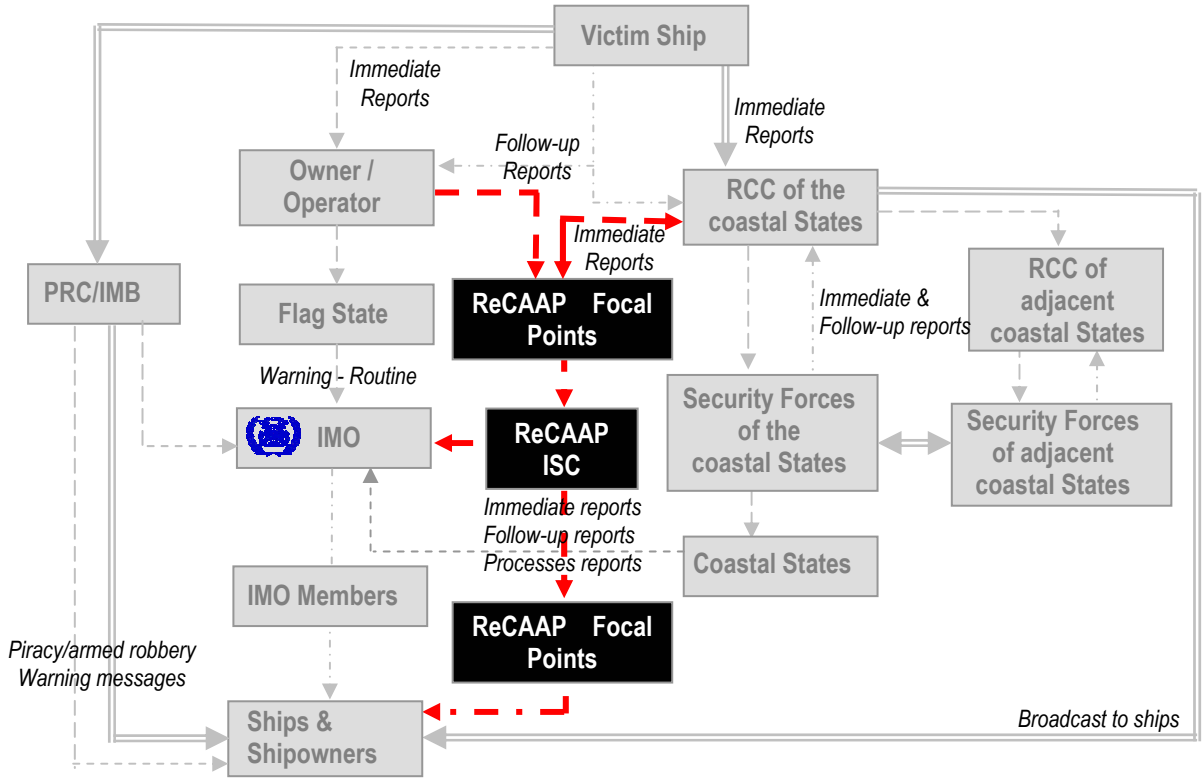
STATISTICS, FLOW DIAGRAMS AND OTHER RELEVANT INFORMATION

Flow diagram for attacks in coastal waters



APPENDIX 2

Flow Diagram for Reporting Incidents in Asia



Legend: Radio/GMDSS :
Fastest means :
Follow-up comms :

Notes:

1. *In the Asian region, the RCCs of some ReCAAP Contracting Parties are also their ReCAAP Focal Points (FPs). These Focal Points also disseminate incident information internally to their respective RCCs, maritime authorities and law enforcement agencies as appropriate.*
2. *Coastal States (in the context of this addendum) refer only to those who are Contracting Parties to the ReCAAP.*
3. *The incident reporting process in Asia does not change other reporting processes for incidents already in practice.*

APPENDIX 3

"PHASES" RELATED TO VOYAGES IN PIRACY AND ARMED ROBBERY THREAT AREAS

Phase Symbol	Phase Description
A	Approaching a piracy/armed robbery threat area (1 hour prior to entering)
B	Entering a piracy/armed robbery threat area
C	Inside a piracy/armed robbery threat area, but no suspect piracy/armed robbery vessel detected
D	Inside a piracy/armed robbery threat area: suspect piracy/armed robbery vessel detected
E	Certainty that piracy/armed robbery will be attempted
F	Pirate/armed robbery vessel in proximity to, or in contact with, own ship
G	Pirates/armed robbers start attempts to enter ship
H	Pirates/armed robbers have succeeded in entering ship
I	Pirates/armed robbers have one or more of the ship's personnel in their control/custody
J	The pirates/armed robbers have gained access to the bridge or the master's office
K	The pirates/armed robbers have stolen property/money, etc.
L	The pirates/armed robbers start to disembark
M	The pirates/armed robbers have disembarked
N	The pirate/armed robbery vessel is no longer in contact with the ship
O	Own ship leaves the piracy/armed robbery threat area

APPENDIX 4

EXTRACT FROM UN GUIDANCE ON SURVIVING AS A HOSTAGE

Introduction

Over the past few years the number of seafarers who have been kidnapped or taken hostage has increased substantially. Every hostage or kidnap situation is different. There are no strict rules of behaviour; however, there are a number of steps which you can take to minimize the effects of detention and enhance your ability to cope and to see the incident through to a successful release.

Survival considerations

These techniques have been successfully employed by others who have been taken hostage:

- No one can tell an individual whether he or she should resist or not if taken hostage/kidnapped. This decision must be made by each person's own assessment of the circumstances. Resisting the attempt may be extremely risky. You may be injured if you attempt to resist armed individuals. It is possible that you will immediately be blindfolded and drugged.

- Being taken hostage is probably one of the most devastating experiences a seafarer can undergo. The first 15 to 45 minutes of a hostage situation are the most dangerous. Follow the instructions of your captors. They are in a highly emotional state, regardless of whether they are psychologically unstable or caught in an untenable situation. They are in a fight or flight reactive state and could strike out. Your job is to survive. After the initial shock wears off, your captors are able to better recognize their position. Be certain you can explain everything on your person.

- Immediately after you have been taken, pause, take a deep breath and try to relax. Fear of death or injury is a normal reaction to this situation. Recognizing your reactions may help you adapt more effectively. A hostage usually experiences greatest anxiety in the hours following the incident. This anxiety will begin to decline when the person realized he/she is still alive – at least for now – and a certain routine sets in. Feelings of depression and helplessness will continue throughout captivity and most hostages will feel deeply humiliated by what they undergo during captivity. Most hostages, however, will quickly adapt to the situation. Remember your responsibility is to survive.

- Do not be a hero; do not talk back or act "tough". Accept your situation. Any action on your part could bring a violent reaction from your captors. Past experiences show that those who react aggressively place themselves at greater risk than those who behave passively.

- Keep a low profile. Avoid appearing to study your abductors, although, to the extent possible, you should make mental notes about their mannerisms, clothes and apparent rank structure. This may help the authorities after your release.

- Be cooperative and obey hostage-takers' demands without appearing either servile or antagonistic. Be conscious of your body language as well as your speech. Respond simply if you are asked questions by the hijackers. Do not say or do anything to arouse the hostility or suspicious of your captors. Do not be argumentative. Act neutral and be a good listener to your captors. Do not speak unless spoken to and then only when necessary. Be cautious about making suggestions to your captors, as you may be held responsible if something you suggest goes wrong.

- Anticipate isolation and possible efforts by the hostage-takers to disorient you. Your watch may be taken away so you are unable to determine whether it is night or day. Nevertheless, try to maintain a routine.

- Try to appear uninterested as to what is going on around you. Sleep, read a book, etc. When so occupied, you will be less influenced by what is going on around you, and hijackers do not bother people who are not a threat to them.

- Try to keep cool by focusing your mind on pleasant scenes or memories or prayers. Try to recall the plots of movies or books. This will keep you mentally active. You must try to think positively. Try to maintain a sense of humour. It will lessen anxiety.

- Ask for anything you need or want (medicines, books, paper). All they can say is no.

- Build rapport with your captors. Find areas of mutual interest which emphasize personal rather than political interests. An excellent topic of discussion is family and children. If you speak their language, use it – it will enhance communications and rapport.

- Bear in mind that hostages often develop a positive attitude towards their captors. This is known as "Stockholm Syndrome", after an incident involving hostages at a Swedish bank. In addition, as the hostage identifies with his/her captors, a negative attitude towards those on the outside may develop.

- You may be asked to sign notes verifying that you are alive or you may be asked to write a "confession" that you or the organization have been involved in nefarious activities. The decision to sign these is an individual one based on the situation. Some hostages refuse to sign unless the language of the note is changed. This may help bolster your morale and make your feel less helpless. It can also serve to command a certain degree of respect from the captors.

- Exercise daily. Develop a daily physical fitness programme and stick to it. Exercises will keep your mind off the incident and will keep your body stimulated. If possible, stay well-groomed and clean.

- As a result of the hostage situation, you may have difficulty retaining fluids and may experience a loss of appetite and weight. Try to drink water and eat even if you are not hungry. It is important to maintain your strength.

- Do not make threats against hostage-takers or give any indication that you would testify against them. If hostage-takers are attempting to conceal their identity, give no indication that you recognize them.

- Try to think of persuasive reasons why hostage-takers should not harm you. Encourage them to let authorities know your whereabouts and condition. Suggest ways in which you may benefit your captors in negotiations that would free you. It is important that your abductors view you as a person worthy of compassion and mercy. Never beg, plead or cry. You must gain your captors' respect as well as sympathy.

- If you end up serving as a negotiator between hostage-takers and authorities, make sure the messages are conveyed accurately. Be prepared to speak on the radio or telephone.

- Escape only if you are sure you will be successful. If you are caught, your captors may use violence to teach you and others a lesson.

- At every opportunity, emphasize that, as a seafarer you are neutral and not involved in politics.

- If there is a rescue attempt by force, drop quickly to the floor and seek cover. Keep your hands over your head. When appropriate, identify yourself. In many cases, former hostages feel bitter about the treatment they receive after their release. Most hostages feel a strong need to tell their story in detail. If assistance in this regard is not provided, request a post-traumatic stress debriefing. Bear in mind that the emotional problems of a former hostage do not appear immediately. Sometimes they appear months later. Whatever happens, readjustment after the incident is a slow process requiring patience and understanding. As soon as the hostage realizes that he or she is a normal person having a normal reaction to an abnormal situation, the healing process can begin.

- Be patient.

APPENDIX 5

SHIPS' MESSAGE FORMATS

Report 1 - Initial message - Piracy/armed robbery attack alert

1 Ship's name and, callsign, IMO number, INMARSAT IDs (plus ocean region code) and MMSI

MAYDAY/DISTRESS ALERT (see note)

URGENCY SIGNAL

PIRACY/ARMED ROBBERY ATTACK

2 Ship's position (and time of position UTC)

Latitude Longitude
Course Speed KTS

3 Nature of event

Note: It is expected that this message will be a Distress Message because the ship or persons will be in grave or imminent danger when under attack. Where this is not the case, the word MAYDAY/DISTRESS ALERT is to be omitted.

Use of distress priority (3) in the INMARSAT system will not require MAYDAY/ DISTRESS ALERT to be included.

Report 2 - Follow-up report - Piracy/armed robbery attack alert

1 Ship's name and, callsign, IMO number

2 Reference initial PIRACY/ARMED ROBBERY ALERT

3 Position of incident
Latitude Longitude
Name of the area

4 Details of incident, e.g.:
While sailing, at anchor or at berth?
Method of attack
Description/number of suspect craft
Number and brief description of pirates/robbers
What kind of weapons did the pirates/robbers carry ?
Any other information (e.g., language spoken)
Injuries to crew and passengers
Damage to ship (Which part of the ship was attacked?)
Brief details of stolen property/cargo
Action taken by the master and crew

Was incident reported to the coastal authority and to whom?
Action taken by the Coastal State

5 Last observed movements of pirate/suspect craft, e.g.:
Date/time/course/position/speed

6 Assistance required

7 Preferred communications with reporting ship, e.g.:
Appropriate Coast Radio Station
HF/MF/VHF
INMARSAT IDs (plus ocean region code)
MMSI

8 Date/time of report (UTC)

APPENDIX 6

FORMAT FOR REPORTING TO IMO THROUGH MARITIME ADMINISTRATIONS OR INTERNATIONAL ORGANIZATIONS

2* Ship's name and IMO number
Type of ship
Flag
Gross tonnage
3 Date and time
4 Latitude Longitude
Name of the area**
While sailing, at anchor or at berth?
5 Method of attack
Description/number of suspect craft
Number and brief description of pirates/robbers
What kind of weapons did the pirates/robbers carry ?
Any other information (e.g., language spoken)
6 Injuries to crew and passengers
Damage to ship (Which part of the ship was attacked?)
Brief details of stolen property/cargo
7 Action taken by the master and crew
8 Was incident reported to the coastal authority and to whom?
9 Reporting State or international organization
10 Action taken by the coastal State

---

* Corresponding to the column numbers in the annex to the IMO monthly circulars

** The following definition of piracy is contained in article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS):

"Piracy consists of any of the following acts:

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

APPENDIX 7

DECALOGUE OF SAFETY

1 Watch over the ship and the cargo

It is the duty of every Master to take care of the cargo and take precautionary measures for the complete safety of the ship, as well as that of the activities carried out on board by the crew or other persons employed on board. All crew members should co-operate in the vigilance, in their own interests, communicating any suspicious activity to the Officer of the Watch.

2 Illuminate the ship and its side

Keep the ship illuminated, particularly, the outer side and the whole length of the deck, using high powered floodlights. Bad visibility impedes the action of the watchmen, constituting a favourable factor for unlawful activities. Do not forget what is recommended in rules 2 and 30 of the COLREG.

3 Establish communication for outside support

Whenever possible, install a telephone line with easy access for the watchman or crew member on duty. Ask for assistance by the telephone.

Remember also the list of stations which will be on permanent watch on VHF - channel 16. These stations can forward the request for assistance to the competent authorities.

4 Control of accesses to the cargo and to living quarters

The Master's cabin is one of the main objectives of the assailants who are looking for money and the master keys to other living quarters, to steal the crew's personal effects of value and nautical equipment from the bridge. The cabins and other living quarters should be kept locked whenever their occupants are absent.

Normally cargo will only be the object of robbery or theft if the criminals have advance knowledge of the contents, through information collected by unscrupulous persons who have access to the bill of lading. Attempt to stow the containers with valuable cargo in a manner to obstruct their doors. Isolate the means of access to the ship and also the accesses to the internal areas, creating a sole way of entry and exit by the gangway, guaranteeing its control by the watchman posted there.

5 Keep the portholes closed

Open portholes can be an easy access to clever criminals: close them with the clips in place always when you leave. Try also to keep the accesses to internal areas locked, guaranteeing the entry and exit by the gangway watchman.

6 Do not leave valuables exposed

Try to reduce the opportunities of robbery by putting all portable equipment which is not in use to its place of storage. Valuables left exposed tempt opportunistic thieves, keep them in safe place under lock and key.

7 Keep the gangways raised

At anchorages and in port, make the access difficult by keeping the gangways and rope ladders raised. In port, only leave the gangway to the dockside down.

8 In case of an assault

I - do not hesitate to sound the ship's general alarm in case of a threat of assault;

II - try to keep adequate lighting to permanently dazzle the opponents, in case of an attempt by strangers to climb the ship's side;

III - raise the alarm, by VHF - channel 16, to the ships in the area and to the permanent watch system of the authorities ashore (cite the existing structure in the port). The efficiency of assistance by the security forces depends on an early alarm;

IV - sound the alarm with intermittent blasts on the siren and use visual alarms with floodlights and signalling rockets;

V - if appropriate, to protect the lives of those onboard, use measures to repel the boarding by employing powerful floodlights for dazzling the aggressors or using jets of water or signalling rockets against the areas of boarding; and

VI - do not attempt any heroic acts.

9 Keep the contracted watchmen under the control of the officer of the watch

Demand a good watchman service. Make them identify all persons that enter and leave the ship. Recommend that the crew co-operate with the control. Do not allow the watchman to leave the gangway, unless he is relieved by another watchman or a crew member.

10 Communicate to the police any occurrence relating to robbery, theft or assault

Occurrences involving assault or robbery should be communicated to the Security forces, for the pertinent legal steps to be taken.

This information will make possible the study of measures to be adopted for the prevention and combat of these crimes, contributing to guaranteeing the safety of the crew and the ship.

_____

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/Rev.1
14 June 2021

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/Circ.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 The Maritime Safety Committee, at its 103rd session (5 to 14 May 2021), approved replacing annex 3 of this circular with revised BMP West Africa guidance, issued by industry in March of 2020.

6 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.

7 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.

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

9 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.

10 This circular and any revisions supersede MSC.1/Circ.1339.

***

Global Counter Piracy Guidance for Companies, Masters and Seafarers

Produced and supported by:

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

Global Counter Piracy Guidance for Companies, Masters and Seafarers

First Published June 2018

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

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

Published by

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

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

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

Contents

Fundamentals

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

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

IF ATTACKERS CANNOT BOARD A SHIP THEY CANNOT HIJACK IT

Aide Memoire

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

Section 1

Introduction

Piracy and Armed Robbery at Sea

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

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

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

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

This guidance consists of:

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

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

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

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

Other sources of information include:

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

UKMTO (www.ukmto.org)

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

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

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

ReCAAP website (www.recaap.org).

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

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

Other Maritime Security Threats

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

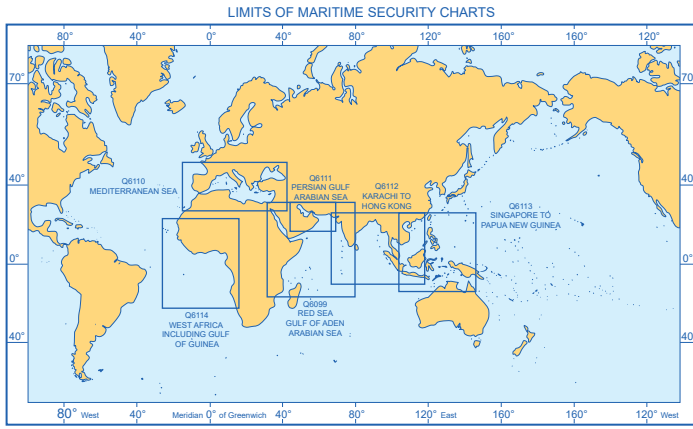
Appendix A provides guidance on other security threats to assist companies, CSOs and Masters in identifying and preparing for other maritime security threats that may be encountered during a voyage, and identifying the resources by which they can assess the risk to the ship and crew and identify measures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

Piracy and Armed Robbery against Ships Worldwide

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

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

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



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

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

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

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

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

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

Joint War Committee Listed Area

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

Voluntary Reporting

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

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

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

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

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

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

Section 4

Company Threat and Risk Assessment

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

Threat Assessment

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

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

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

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

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

Risk Assessment

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

4.1 Risk assessment considerations for the Company

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

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

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

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

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

Section 5

Company Planning

5.1 Company planning prior to entering an area of increased risk

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

5.1.1 Register ship with relevant reporting centre

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

5.1.2 Obtain latest threat and risk information from designated regional sources

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

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

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

5.1.4 Put ship protection measures in place

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

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

5.1.5 Monitor piracy related websites for current threats

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

5.1.6 Offer guidance to the Master as to recommended route

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

5.1.7 Plan to maintain security of critical information

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

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

5.2 Company planning on entering an area of increased risk

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

Section 6

Ship Master's Planning

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

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

6.1.1 Implement SPMs

SPMs should be implemented as determined through the risk assessment.

6.1.2 Brief crew, check equipment and conduct drills

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

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

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

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

6.1.3 Emergency Communication Plan

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

6.1.4 Automatic Identification System

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

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

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

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

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

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

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

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

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

6.2.1 Submit initial Ship Position Report Form

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

6.2.2 Implement the measures required by the risk assessment

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

6.2.3 Implement the Communications Policy

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

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

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

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

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

6.2.5 Carefully review all warnings and information

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

6.2.6 Consider speed and manoeuvring

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

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

Freeboard

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

Location and Time at Anchor

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

Coordinated Arrival

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

Sea State

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

6.2.7 Increase vigilance during STS/SBM operations

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

6.2.8 Submit daily position report to relevant reporting centre

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

6.2.9 Consider utilisation of Convoy systems where available

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

Section 7

Ship Protection Measures (SPM)

7.1 Introduction

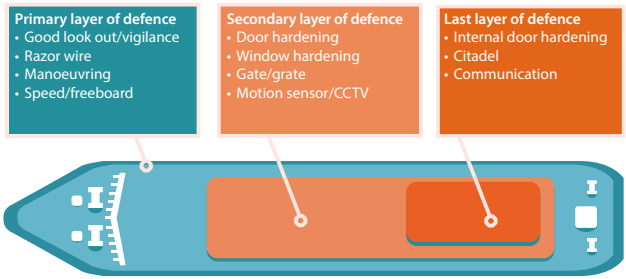
This section focuses on measures that can be taken by the ship's crew to mitigate against attack.

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

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

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

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



An example of "layered" defence

7.2 Watch keeping and enhanced vigilance

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

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

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

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

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

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

7.3 Enhanced bridge protection

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

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

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

7.4 Control of access to bridge, accommodation and machinery spaces

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

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

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

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

7.5 Physical barriers

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

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

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

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

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

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

7.6 Water spray and foam monitors

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

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

The following points are relevant:

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

7.7 Alarms

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

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

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

7.8 Manoeuvring practice

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

7.9 Closed circuit television

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

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

7.10 Lighting

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

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

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

7.11 Secure storage of ship's tools and equipment

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

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

7.12 Safe muster points and citadels

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

7.12.1 Safe muster points

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

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

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

7.12.2 Citadels

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

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

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

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

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

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

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

7.13 STS and other static operations

Attackers have boarded ships on STS operations via the fenders.

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

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

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

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

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

Other considerations for the Master during STS or static operations:

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

7.14 Unarmed Private Maritime Security Contractors

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

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

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

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

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

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

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

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

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

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

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

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

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

7.16 Vessel Protection Detachments (VPDs)

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

Action on Attack and/ or Boarding

8.1 General

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

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

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

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

8.2 Suspicious approach

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

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

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

8.3 When under attack

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

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

8.4 Action if the ship is boarded

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

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

8.5 Action if attackers take control

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

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

8.6 Kidnap

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

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

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

DO NOT:

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

DO:

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

8.7 In the event of military action

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

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

Section 9

Post Incident Reporting

9.1 General

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

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

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

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

9.2 Investigation

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

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

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

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

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

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

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

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

9.3 Reports

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

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

9.4 Advice

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

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

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

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

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

Section 10

Humanitarian Considerations

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

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

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

List of Abbreviations

AIS – Automatic Identification System

BAM – Bab al-Mandeb

CCTV – Closed Circuit Television

CMF – Combined Military Forces

CSO – Company Security Officer

EUNAVFOR – European Naval Forces Operation Atalanta

GoG – Gulf of Guinea

GoO – Gulf of Oman

IFC – Information Fusion Centre Singapore

IMB – International Maritime Bureau

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

IMO – International Maritime Organization

IRTA – Industry Releasable Threat Assessment

IRTB – Industry Releasable Threat Bulletin

ISPS Code – International Ship and Port Facility Security Code

JWC – Lloyd's Joint War Committee

MARSEC Level – Maritime Security Level

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

MRCC – Maritime Rescue Coordination Centre

MSCHOA – Maritime Security Horn of Africa

NAVWARN – Navigation Warning

PA System – Public Address System

PCASP – Privately Contracted Armed Security Personnel

PMSC – Private Maritime Security Companies

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

RUF – Rules for the Use of Force

SEA – South East Asia

SPMs – Ship Protection Measures

SSAS – Ship Security Alert System

SSP – Ship Security Plan

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

UKMTO – United Kingdom Maritime Trade Operations

VHF – Very High Frequency

VPD – Vessel Protection Detachment

VRA – Voluntary Reporting Area

WIO – Western Indian Ocean

Appendix A

Other Maritime Security Threats

1. Introduction

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

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

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

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

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

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

3.1 Terrorism

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

3.2 War and warlike activity

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

3.3 Cyber attacks

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

4. ISPS Code

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

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

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

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

5. Identifying and Preparing for Other Maritime Security Threats

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

5.1 Threat and risk assessment

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

5.2 Company and Master's planning

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

5.3 Ship protection measures

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

5.4 Brief crew, check equipment and conduct drills

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

5.5 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

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

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, CLIK, 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, OCIMF, Sailors' Society, SIGTTO, World Shipping Council, CONTACT GROUP ON PIRACY OFF THE COAST OF SOMALIA, EU NAVFOR Somalia, MARITIME, ICC International Maritime Bureau, 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

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

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.

ANNEX 2

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.

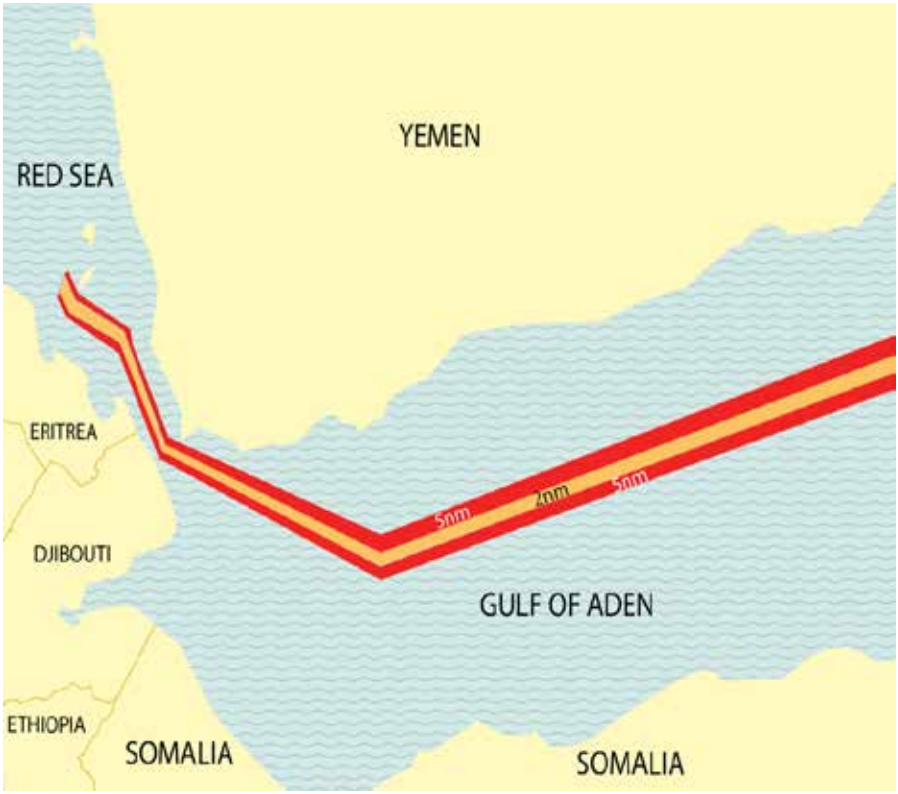
Maritime Security Transit Corridor

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.

ANNEX 2



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.

ANNEX 2

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.

ANNEX 2

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.

ANNEX 2

On entering the High Risk Area

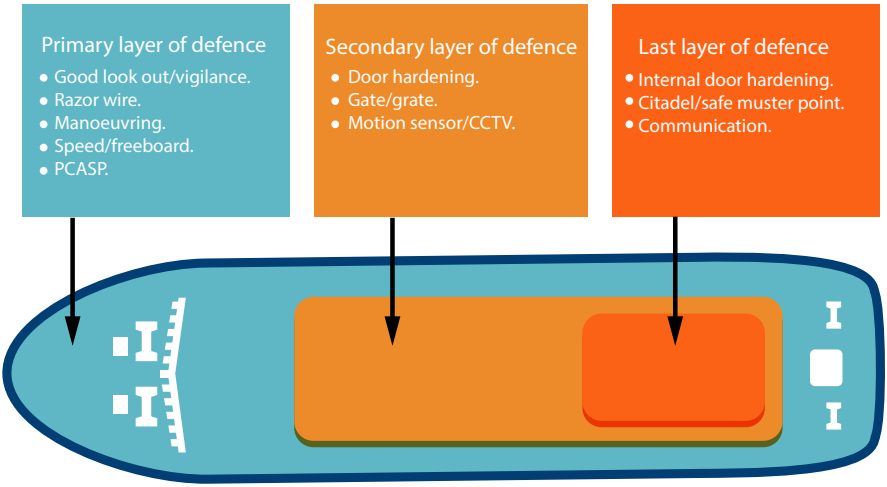
- Submit ship reports as highlighted in section 6 and annexes D and E.
- Monitor latest threat information.
- Ensure all access points are limited and controlled.
- Avoid drifting, waiting, anchoring and slow steaming, particularly in the MSTC.
- Minimise use of VHF and use email or a secure satellite 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.

ANNEX 2

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.

ANNEX 2

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.

ANNEX 2

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.

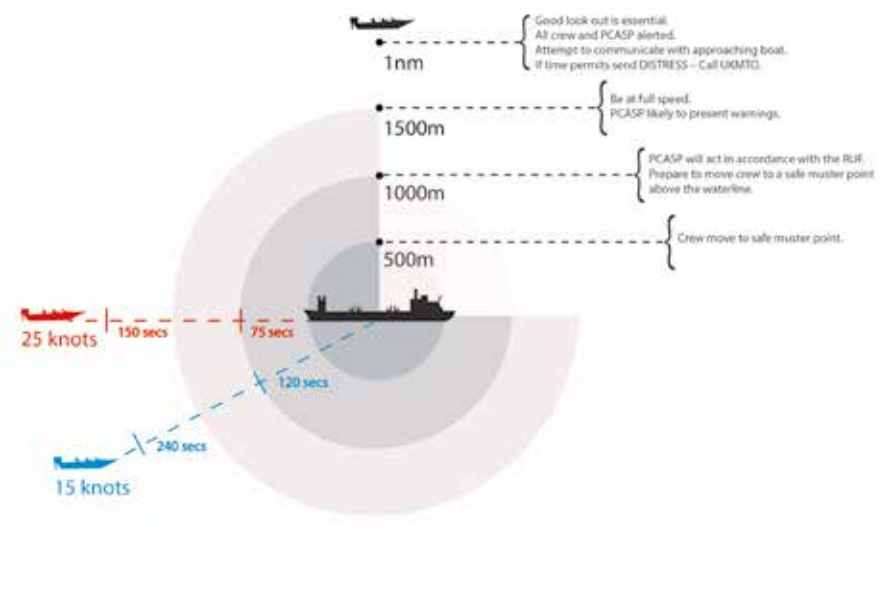
Attack from other threats

- **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.

ANNEX 2

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

ANNEX 2

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

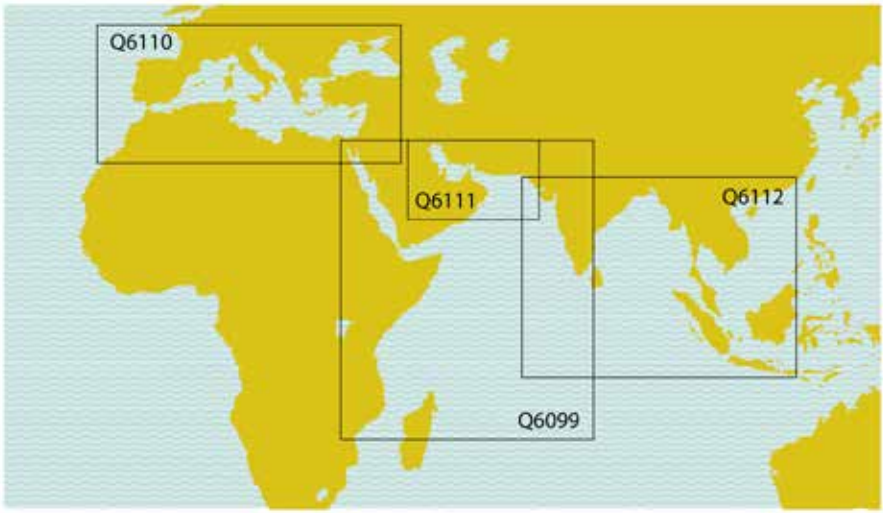
Email	info@recaap.org
Telephone	+65 6376 3063
Fax No	+65 6376 3066

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

ANNEX 2

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.

ANNEX 2

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

ANNEX 2

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

ANNEX 2

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 Pandl 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

ANNEX 2

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

ANNEX 2

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.

ANNEX 2

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.

ANNEX 2

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

BMP West Africa

Best Management Practices to Deter Piracy and Enhance Maritime Security off the Coast of West Africa including the Gulf of Guinea

Produced and supported by:

BIMCO · CDI · CLIA · ICC International Maritime Bureau · IFC · IFSMA · IGP&I International Group of P&I Clubs · IMCA · IMEC · INTERCARGO · InterManager · International Chamber of Shipping · INTERPOL · INTERTANKO · IPTA International Parcel Tankers Association · itf · ISWAN · Joint Hull Committee · Joint War Committee · OCIMF · Sailors' Society · SIGTTO · The Mission to Seafarers · WORLD SHIPPING COUNCIL PARTNERS IN TRADE

BMP West Africa

Best Management Practices to Deter Piracy and Enhance Maritime Security off the Coast of West Africa including the Gulf of Guinea

Version 1 published March 2020

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

Contents

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, insurance and military guidance.

Report

- Register and report to MDAT-GoG.
- 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

The maritime security situation off the West Coast of Africa is complex and dynamic. BMP – West Africa (WA) has been produced to help ships and seafarers avoid becoming the victims of maritime security incidents in these waters.

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

The BMP contained in this publication mitigate the risk from piracy and armed robbery. However, differences in attack methods from other threats may require other forms of mitigation.

The consequences of not adopting effective security measures can be severe. Some pirates have subjected crew to violence and other ill treatment and extended periods of captivity. Other attacks have demonstrated an intent to damage ships, seize the cargo and endanger life.

Other maritime crime in the region, such as the trafficking of firearms, humans and narcotics, migrant smuggling and illegal, unreported and unregulated (IUU) fishing, can contribute to insecurity.

The Maritime Domain Awareness for Trade-Gulf of Guinea (MDAT-GoG) (**https://gog-mdat.org/home**) website should be consulted for advice. See annex A for contact details.

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

This BMP complements piracy guidance in the latest International Maritime Organisation (IMO) Resolutions and Circulars (**www.imo.org**).

Geographical area

This Guidance introduces recommended practices and procedures for vessels operating in the Voluntary Reporting Area as depicted on UKHO Chart Q6114 and SHOM Chart 8801CSD.

Attacks on ships and seafarers have taken place throughout the region but most predominantly in the eastern part of the Gulf of Guinea. Threats are dynamic; information should be sought from the organisations listed in annex A.

Voluntary Reporting Area

The MDAT-GoG Voluntary Reporting Area (VRA) is identified on maritime security charts such as **UKHO Q6114** & **SHOM Chart 8801CSD.** Ships entering and operating within the VRA are encouraged to register with the MDAT-GoG as registration establishes direct contact between the reporting ship and MDAT-GoG.

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 the JWC listed area can be found on their website: **www.lmalloyds.com/lma/jointwar**

Section 2

The threat

The complex range of maritime security issues off the coast of West Africa creates direct and indirect threats to the safety of seafarers. For this reason, it is important that all maritime crime is addressed. This Guidance focuses on maritime crime that causes a direct threat to seafarers, armed (and unarmed) robbery, including cargo theft, hijacking of vessels and kidnapping.

The likelihood of attack further offshore is higher during the inter-monsoon season (September-March). Attacks can take place at any time – day or night. However, more seafarers have been kidnapped during the hours of darkness.

Attacks on Vessels

Attacks occur close to shore, in rivers and in ports; however, attacks have been reported over 200Nm from the coast.

Attacks on vessels vary significantly in their form. Attacks for theft may involve just a few individuals. However, an attack on a vessel where the intention is the kidnapping of seafarers and/or offloading cargo from tankers may involve a large number of heavily armed individuals. Different types of vessels are used during attacks, these include fast small craft, fishing vessels and small merchant vessels. Whilst most attacks on ships at anchor off ports occur at night, many of the attacks further out to sea occur during the day or night. Ships at anchor, drifting or conducting ship-to-ship (STS) operations are particularly vulnerable. Attacks against vessels underway may occur when proceeding at slow speed and occasionally involve some form of deception to force the vessel to stop. If a mother ship is used it will carry pirates, stores, fuel and attack skiffs to enable attackers to operate over a much larger area.

Attackers may use small arms fire and Rocket Propelled Grenades (RPGs) during attacks; the bridge and accommodation tend to be the main targets for these weapons. Attackers may 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 others to board.

The objective of an attack varies. Kidnap for ransom is widespread. These kidnappings have ranged from one seafarer to the entire crew of a ship. Seafarers are held in distressful, unsanitary conditions lacking adequate medical support, which has resulted in sickness and sometimes death.

Cases of armed robbery at sea involve the theft of cargo, valuables and the destruction of navigation and communication equipment; sometimes they are opportunistic but are carefully planned. A hijack will typically last several days whilst the vessel is moved around outside the jurisdiction of the coastal states. During this time the vessel may be moved to a number of rendezvous points to enable STS transfers of cargo.

Experience has shown the crew of a vessel targeted for armed robbery at sea or cargo theft are likely to be treated badly by perpetrators during an attack. Injuries are common and any resistance shown to the attackers may lead to an escalation of violence.

The capability of military and law enforcement forces to respond to incidents of armed robbery at sea, hijacking and kidnapping in the Voluntary Reporting Area (VRA) is improving, but remains limited. Only a few countries provide or allow Secure Anchorage Areas (SAA), Security Escort Vessels (SEV) and or Vessel Protection Detachments (VPDs) for merchant vessels within their EEZ and/or territorial waters.

Other maritime security concerns are outlined at annex E.

Section 3

Threat and risk assessment

Threat assessment

The threat assessment must include all regional maritime security threats.

As part of every ship risk assessment prior to transit through the VRA the latest regional threat advice can be obtained from the Interregional Coordination Centre, MDAT-GoG, the IMB Piracy Reporting Centre (IMB PRC) and commercial providers.

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 or by good intelligence. 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 specific threat 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.

Further guidance on risk assessments can be found at **www.maritimeglobalsecurity.org**

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

- The threat assessment and geographical areas of increased risk.
- Requirements of the Flag State, company, charterers and insurers.
- Secure Anchorage Areas (SAA), Security Escort Vessels (SEV) and or Vessel Protection Detachments (VPDs).
- 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).
- Background factors shaping the situation, e.g. traffic patterns and local patterns of life, including fishing vessel activity.
- Cooperation with military.

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 and any rendezvous requirements.
- Due diligence of companies providing security services.
- Guidance on using a SAA, SEV and any transfer to terminal security.
- Company mandated Ship Protection Measures (SPM).
- Companies should consider using hidden position transmitting devices as hijackers will often attempt to disable all visible communication and tracking devices and aerials straight away.
- Review of company manning requirements. Consider disembarking of non- essential crew and families prior to sailing to areas of high security risk.
- 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.
- Minimise the use of VHF and use email or a secure satellite telephone instead. Where possible, only answer known or legitimate callers on the VHF and keep voyage critical information to a minimum.
- Email correspondence to agents, charterers and chandlers should be controlled and information within the email kept concise, containing the minimum that is contractually required.
- Reminding crew of the dangers of posting voyage related information on social media.

STS Operations

- Review the threat assessment and security measures for the location of STS operations.

Offshore Terminals

- Review the threat assessment and security measures for the location of Offshore Terminals.

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, alerts and the Inmarsat SafetyNet broadcasts.
- Implement VRA vessel registration and reporting requirements as highlighted in section 6 and annex D.
- If security services are used, confirm arrangements with the Private Maritime Security Companies (PMSC).
- If used, rendezvous position and communication plan for Security Escort Vessels.
- Contingency plans if security services do not arrive or cannot meet operational requirements.
- Confirm propulsion can operate at full speed.
- Implement security measures in accordance with the Ship Security Plan (SSP).

Brief crew and conduct drills

Crews should be made aware of the threat, risk and consequences along with available resources to cope. Good practice guides can be found at **https://www.seafarerswelfare.org/resources**

The crew should be fully briefed on the preparations and drills should be conducted with the Ship Protection Measures (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 and crew awareness.
- The crew's understanding of required action in the event of an attack.

On entering the VRA

- Submit ship reports as highlighted in section 6 and annex D.
- Update and monitor latest threat information.
- Ensure all access points are limited and controlled.
- Minimise the use of VHF and use email or a secure satellite telephone instead. Where possible, only answer known or legitimate callers on the VHF and keep ship, crew, cargo and voyage-critical information to a minimum.

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 in the VRA to ensure reporting centres and militaries can track the ship but restrict the data to ship's identity, position, course, speed, navigational status and safety related information.
- Reschedule planned maintenance on voyage critical equipment for transit through areas identified in the risk assessment and have all equipment ready in the event of attack.

Location and Time at Anchor

- Keep time at anchor to a minimum.
- Anchor watch to be maintained.
- Avoid setting patterns.
- Consider use of "secure anchorage areas" operated by some countries in the region. More information is contained in local Notice to Mariners or Admiralty Charts.
- Vessels are most vulnerable when stopped in the water, drifting, at anchor or carrying out STS transfer, Single Buoy Mooring (SBM) operations or slowing down for pilot transfer.

Coordinated Arrival

Many vessels wait offshore and transit at high speed to arrive at any rendezvous point 'Just in Time' including STS and/or Offshore Terminals. Some vessels tender a virtual Notice of Readiness (NOR) whilst staying safely offshore, and both are accepted practice for many vessels operating in the GoG.

Planning considerations for vessels permanently operating inside the VRA

Marine operations in the GoG region are diverse, covering many areas of activity including:

- Offshore supply.
- Diving & RoV Support.
- MODU/MOU.
- Pipe laying.
- Fishing vessels.
- Passenger vessels and ferries.
- Recreation craft.

In general, maritime security considerations for vessels permanently operating in the region are not dissimilar to those for vessels visiting the region, its ports and harbours.

There is no set pattern to the location of attacks against vessels based and operating in the region, but it should be assumed criminals are aware of the regular transit routes to offshore installations, STS and ship waiting areas, fishing grounds and scheduled ferry routes.

Section 5

Ship Protection Measures

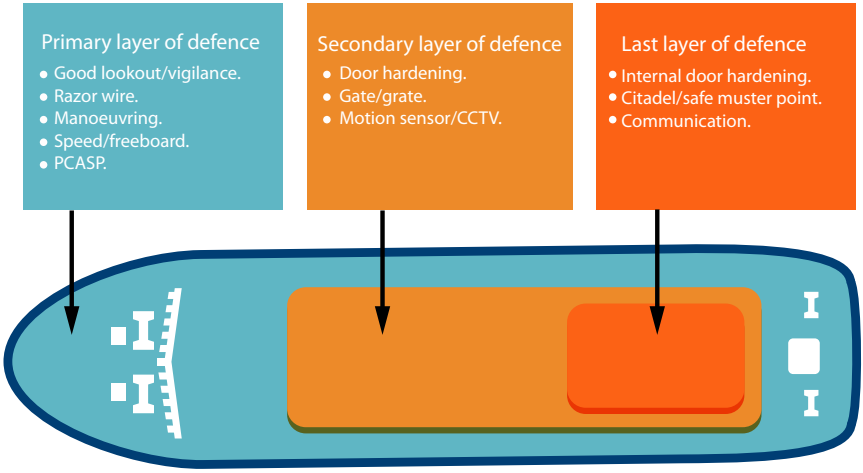
This section highlights proven SPM that provide layered protection. The BMP is based on regional experience of attacks and will continue to evolve as methods change.

When considering SPM it is important to recognise that ships may be subject to attack whilst underway or stationary. Ships are especially vulnerable when at anchor or when carrying out STS or SBM operations.

A Vessel Hardening Plan (VHP) can ensure vessels are prepared for operations in areas of increased threat and ought to be considered as part of voyage preparation. The requirement for a VHP should be defined within the company management procedures for security. The Company Security Officer (CSO) should be responsible for the plan, with the Master and Ship Security Officer (SSO) reviewing the contents before transit or operation within known security risk areas.

The implementation of SPM will be identified during the voyage planning process and clearly marked on the VHP. 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. During STS operations there is a tendency for members of the crew to be looking “in” not “out”.
- Enhanced vigilance may be required for exposed fender and mooring stations where SPM have been removed.
- 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 safety 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.
- Consider mounting anti-piracy mirrors on the bridge wings to make looking aft easier.
- The accommodation and pilot ladders, if rigged, should be kept at main deck level and lowered when required only.
- When in port:
  - Access to the vessel must be controlled.
  - Regular security rounds should be conducted.

- Ensure the crew, especially those assigned to Security Duties are well rested.

A proper 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 the effect of hydrostatic pressure between vessels can have a better defensive impact than speed.

Alarms

The ship's alarms inform the 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. When planning the placement of barriers, special consideration should be given to ships with sunken poop decks.

Razor wire

Razor wire creates an effective barrier only 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 or chafe mooring ropes.

Other physical barriers

Other barriers have proven effective – from hanging swinging obstacles over the gunwales to specifically designed overhanging protection that prevents 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 firefighting 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.
- The vulnerability of bridge doors should be considered. Any physical barrier should not impede access to life saving appliances.

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 that it can be opened from the inside. Where the door or hatch is locked, it is essential that 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 storerooms 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. Experience shows these safe areas are effective.

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.
- An area where crew not required on the bridge or the engine room control room will muster if the ship is under threat.
- A short-term safe haven, which will provide protection should the attackers commence firing weapons.

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 include a lockdown plan and procedures 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.

Citadel Management

The decision to send the crew to the citadel rests with the Master of the vessel. When considering the use of a citadel in the Gulf of Guinea it is important to consider how and when the crew exit the citadel and regain control of the vessel once the perpetrators have left. Experience has shown rescue forces are unlikely to arrive before the perpetrators have left the vessel or may not arrive at all.

Planning Considerations

- If military or law enforcement do not respond to an incident, is a plan in place for exiting the citadel?
- To aid situational awareness on the vessel:
  - A CCTV feed in the citadel can provide awareness of activity on the vessel.
  - Transmit the vessel's CCTV feed to Company HQ who can monitor and advise when safe to leave the citadel.
  - Ensure contact details for company, Flag State and MDAT-GoG are available in 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 closed circuit television (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. The ability to turn off all internal accommodation lights to deter pirates from entering or disorientate those who may already have entered. The following is recommended:

Underway

- At night, only navigation lights should be exhibited and remain on at all times.
- If fitted, search lights should be 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 anchor

- At anchor, lights should be left on as well-lit ships are less vulnerable to attack.
- Over side lighting should be kept on at all times during hours of darkness.

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.

Ship-to-Ship operations

- For vessels involved in STS operations, attackers have boarded via the Yokohama fenders. When rigging or tending fenders, razor wire may well interfere with operational requirements.
- The use of a chain link fence, particularly if topped with razor wire, attached to the ship's side rails and supplemented by stanchions in the vicinity of the Yokohama 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 Yokohama fenders, and ship's fairleads could be the use of water spray.
- The hawse pipe should be properly secured to prevent unauthorised 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.
- Crew engaged in security duties should not be given other responsibilities.

Floating (Production) Storage & Offloading (F(P)SO) – Security Measures

F(P)SOs and vessels supporting offshore facilities are vulnerable.

F(P)SO Maritime Safety Zone

Procedures for establishing a vessel safety zone surrounding the F(P)SO that is monitored and continuously controlled for unauthorised vessel entry should be in place. These procedures should include communication checkpoints, means for vessel identification/validation prior approval for entry. UNCLOS article 60.5 should be referenced. Preferably, all vessels approaching within 2NM are monitored and then communicated with/challenged/validated prior to entering in 1NM of the Safety Zone.

There should be means to continuously monitor and detect vessels approaching the F(P)SO's Safety Zone. These may include:

- A proper radar watch.
- 360 degree CCTV coverage of F(P)SO surroundings with thermal imaging target detection/alarming for night time surveillance.
- Dedicated security vessel(s) for continuous patrol and surveillance.

F(P)SO Security Plan

The Security Plan should include:

- Management roles, responsibilities and clearly defined actions taken for threat level and escalation.
- Compliance with measures to enhance maritime security as detailed in the International Convention for the Safety of Life at Sea (SOLAS) 1974 (as amended) and Parts A/B of the ISPS Code.

F(P)SOs not required to comply with the SOLAS and ISPS Code requirements should still consider them when developing security plans.

F(P)SO Access Control

Procedures for controlling access should be established and should consider:

- Induction/familiarisation briefing.
- Designation and marking of areas restricted to authorised personnel.
- System for monitoring physical control and access barriers.
- Identity verification of F(P)SO personnel, contractors, vessel staff and visitors.
- Personnel safety and security requirement briefings.

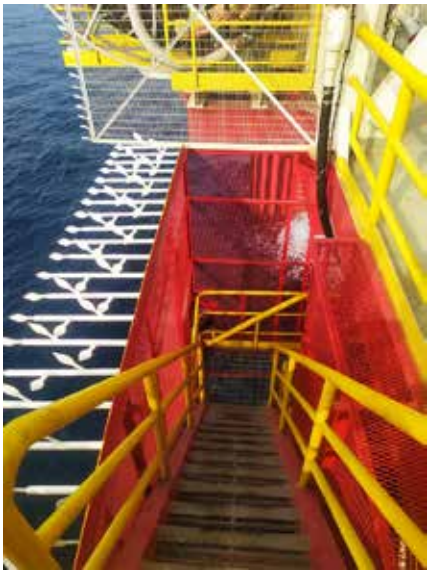
F(P)SO Perimeter Detection Systems

Perimeter and access points from the water such as boat landings and stair towers, as well as vulnerable areas such as mooring chain fairleads, tanker hawser and marine hose connections and riser porches should be equipped with threat detection and deterrent equipment such as:

- 360 degree perimeter lighting.
- CCTV coverage with thermal imaging target detection/alarming.
- Electronic motion detection with visual and audible alarm.

- Depending on threat level – dedicated security person(s) posted to monitor and detect threats by sight and or through threat detection equipment.
- Search lighting (spotlights) capable of scanning 365 degrees of F(P)SO's surrounding waters. Spot light control can be locally but preferably controlled remotely.

F(P)SO Barriers



Perimeter

Vulnerable access points should be equipped with physical hard barriers such as:

- Security fencing and hard bars.
- Razor or concertina wire.

Accommodation, Control Room and Machinery Spaces

Hard barriers for access points including port holes/window glass may include:

- Doors without windows being internally secured.
- Personnel access points being limited to single point of entry and secured during night time operations.
- All windows/port holes secured to prevent access if glass can be broken.
- All cargo and machinery hatches locked internally and easy to unlock in an emergency.

F(P)SO Citadel

F(P)SOs should have a centralised, hardened safe haven (citadel). The citadel should be:

- A hardened room that prevents penetration by small firearms and forceful entry.
- Big enough to safely accommodate all personnel on board.
- Free of dangerous fire suppression systems (CO2).
- Equipped with internal and external communications.
- Supplied with water, medical and toilet facilities.
- Able to access security CCTV and F(P)SO Emergency Shut Down and emergency systems controls.

Private Maritime Security Companies (PMSC)

PMSCs may offer security services and the provision of Security Escort Vessels (SEVs).

BMP does not recommend or endorse the general use of a PMSC or the use of SEVs. This is a decision taken by individual ship operators after carrying out a thorough risk assessment and in conjunction with permissions from the ship's Flag State, the hull and cargo insurance, P&I club and any littoral states.

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

- Coastal state legislation and law enforcement practices.
- The threat and risk environment.
- The output of the company risk assessment.
- Voyage plan requirements.
- Type of operations, e.g. seismic survey or cable laying.
- Levels of protection provided by navies, coastguards and maritime police.

Security Escort Vessels

BMP does not recommend or endorse the general use of SEVs to accompany merchant ships; this is a decision taken by individual ship operators.

A contract for the provision of SEVs must:

- 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.
- Ensure the PMSC can legally operate the SEV in accordance with coastal state law.
- Ensure the SEV is fit for purpose.

Experience has shown some providers operate substandard SEVs. Therefore, any decision to engage the services of SEVs should consider the guidance above for PMSC as well ensuring the vessel operator:

- Has a robust quality assurance programme;
- A robust maintenance programme and;
- A record of inspection.

Companies should check the credentials and licences/ permits of the PMSC.

Operating with Security Escort Vessels

- The escort plan, RV position and communication arrangements should be agreed in advance.
- Planning should consider that SEVs may have operating restrictions.
- Regular communication should be maintained.
- The SEV will be positioned to defend the vessel at all times and be reactive to intercept any approaching suspicious craft.
- Authorisation to use force rests with the military detachment onboard the SEV.
- The Master/Bridge Crew can aid the SEV with early detection and warning.
- SEV should not enter any designated oil terminal exclusion zone.

Section 6

Reporting

All ships using the VRA are strongly encouraged to inform MDAT-GoG 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 annex D are adopted to ensure common understanding.

MDAT-GoG

MDAT-GoG acts as the primary point of contact for merchant ships and their CSOs, providing liaison with military forces in the region. MDAT-GoG 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).

MDAT-GoG 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 MDAT-GoG 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.

MDAT-GoG offers regular information to ships on its website **https://gog-mdat.org/home** and in a weekly report summarising the previous week's activity. MDAT-GoG can offer Masters and CSOs the opportunity to conduct drills and exercises to support their passage planning in the region. Companies interested in this can make contact on a dedicated exercise line; +33 298 221302.

Ships and their operators should submit vessel position reporting forms to MDAT-GoG.

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.

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 MDAT-GoG

MDAT-GoG and the Inter-regional Coordination Centre (ICC) 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. Suspicious activity/attack reports should be sent to MDAT-GoG at the earliest opportunity, to allow assistance to be sought.

MDAT-GoG 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.

Reporting specific vessel sightings and/or activity as requested to MDAT-GoG

MDAT-GoG may seek the assistance of vessels reporting to the centre to try to locate specific ships. These are usually vessels that cannot be found on electronic systems such as AIS. Sometimes the request for information will come directly from MDAT-GoG when, for example, a vessel may have been hijacked and its whereabouts unknown. On other occasions MDAT-GoG may be requested to assist in locating a vessel or seek further information on a vessel by INTERPOL, when an INTERPOL “Purple Notice” has been issued. When MDAT-GoG is seeking further information on a vessel it will contact vessels reporting to it in the VRA for support.

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.

Mother ships

Mother ships have been used in the GoG acting as a base to launch and resupply pirate skiff operations. Mother ships can vary in vessel type and have included offshore supply vessels, fishing vessels or other smaller merchant vessels. Caution must be taken when detecting merchant ships drifting in the area.

Piracy or armed robbery attacks

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

Use whatever time is 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 MDAT-GoG without delay.

Approach stage

Effective lookouts, using all available means, will aid in the early identification of an approaching threat. The nature and intention of the suspicious vessel will only become apparent as it approaches.

In all cases, the following steps should be taken:

- 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.
- If not already at full speed, increase to maximum to open the distance.
- Steer a straight course to achieve maximum speed quickly.
- Initiate the ship's emergency procedures.
- Activate the emergency communication plan.

Report the attack immediately to MDAT-GoG by telephone +33 298 228888 and email **watchkeepers@mdat-gog.org**

- 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 and navigational 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 and the data saved.

Attack stage

As the attackers get close to the ship, the following steps should be taken:

- Reconfirm all ship's crew are in the safe muster point or citadel as instructed by the Master.
- Report the attack immediately to **MDAT-GoG +33 298 228888** 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.
- SEV if present, will conduct themselves as governed by their rules of engagement.

Actions on illegal boarding

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

- Take all way off the ship and then stop the engines.
- Muster the crew in the citadel or safe muster point.
- Use all available means to establish communications from the citadel with MDAT-GoG and company to 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 as advised by the military or company.
- If any member of the crew is captured it should be considered that the attackers 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 eat and drink when offered.
DO take essential medical supplies if moved ashore.

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.

Kidnap and ransom

One reason for attacking a ship off West Africa is to remove the crew ashore for ransom.

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

If kidnapped

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

On receipt of information involving an attack or attempted attack on a vessel or offshore platform, the MDAT-GoG/Regional reporting Centres/IMB PRC will immediately inform all relevant regional and national Maritime Operation Centres who may respond if the incident is within their area of jurisdiction and authority.

Reporting Centres do not have inherent response capability or the ability or mandate to coordinate any response activity, especially inside a nation's territorial waters. This is the responsibility of the national authority with jurisdiction in the area. On the high seas, activities may be coordinated by national authorities. For this reason, reporting any suspicious/attempted or actual approach/attacks immediately to MDAT-GoG/Regional reporting Centres/IMB PRC, using all available means, is important.

Advance warning of military or law enforcement intervention may be difficult without detection and may add pressure on the crew. If the onset of military or law enforcement action is suspected, the following should be considered:

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

Post incident actions and reporting

A difficult period may follow an attack, as companies, Master and crew recover from the ordeal. It is important that seafarers receive timely and proper medical assessments and care, both physical and mental, following an attack or hostage situation. Companies should have emergency management plans in place to manage the effects of 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

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.

Thorough investigation using all available evidence is critical.

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.

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

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 as soon as possible and certainly within three days of a hijacking of their ship.

INTERPOL may also be consulted to discuss recommended practices for the preservation of evidence that could be useful to law enforcement agents pursuing an investigation. Contact details are: **os-ccc@interpol.int**; +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 are a range of humanitarian programmes aimed at assisting seafarers and their families affected 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**

After care of seafarers suffering violent attack is important and should not be neglected.

Annex A

Contact details

Emergency contacts

MDAT-GoG

Email	watchkeepers@mdat-gog.org
Telephone (24hrs)	+33 298 228888
Website	https://gog-mdat.org/home

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

Useful contacts

INTERPOL Command and Coordination Centre

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

Yaoundé Principal Centres

ICC

Email	info@icc-gog.org
Telephone	+237 696281947
	+237 222217529
	(From Monday to Friday, 0830 hours to 1800 (local)

ANGOLA

Luanda Maritime Rescue Coordination Centre (MRCC)

Email	kangamiala@hotmail.com
Telephone	+244 2 2239 1399
	+ 244 2 2233 0430

LIBERIA

Monrovia Regional Maritime Rescue Coordination Centre (RMRCC)

Email	mrcc.monrovia@yahoo.com
IOR INMARSAT C Terminal One	#463728971
AOR-E INMARSAT C Terminal Two	#463728972
INMARSAT Satellite Phone (EXPLORER 710)	#+870772700138
INMARSAT Satellite Phone (EXPLORER 700)	#+870772700139
International Landline	#(+231) 777 092229
International Cellular & SMS	#(+231) 777 290158
Safety & Security Coordination	VHF/DSC CH 16 (Distress) CH 09 (Ship/Shore)
Maritime Security (RMRCC & Liberia CG)	CH 14

Monrovia covers the territorial waters of Liberia and her neighbouring countries – Guinea, Ghana, Liberia, Sierra Leone and Cote d'Ivoire

MOROCCO

Rabat Regional Maritime Rescue Coordination Centre (MRCC)

Email	mrcc.rabat@mpm.gov.mg
Telephone Emergency	+ 212 5 37 625877
Other	+ 212 5 37 625897

Rabat covers the territorial waters of Morocco, Senegal, Mauritania, Guinea Bissau, Gambia and Cape Verde

NIGERIA

Lagos Regional Maritime Rescue Coordination Centre (RMRCC)/C4I Centre

Email	rmrccnigeria@yahoo.com
Telephone (24hrs)	+234 (1) 730 6618, +234 (1) 7053794383

The RMRCC Lagos covers nine countries (Benin, Cameroon, Republic of Congo, the Democratic Republic of Congo, Equatorial Guinea, Gabon, Nigeria, São Tomé & Príncipe and Togo). The RMRCC is collocated with the Nigerian Deep Blue Project C4I Centre.

SOUTH AFRICA

Cape Town Maritime Rescue Coordination Centre (MRCC)

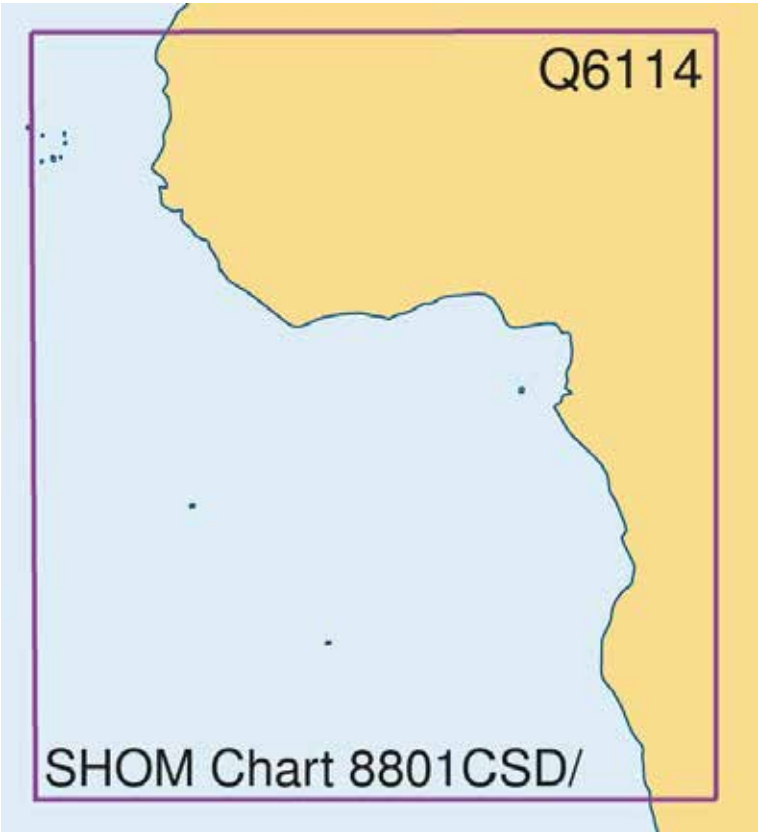
Email	mrcc.ct@samsa.org.za
Telephone	+ 27 21 938 3300 / + 27 21 938 3309

International Seafarers Welfare and Assistance Network (ISWAN)

Email	iswan@iswan.org.uk
Telephone	+44(0) 300 012 4279
Website	www.seafarerswelfare.org

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 UK Hydrographic Office (UKHO) ensuring each chart has the most accurate, up-to-date and verified information available.

The Security Chart for West Africa is the latest version of UKHO Chart Q6114 or SHOM Chart 8801CSD.

Each maritime security chart includes:

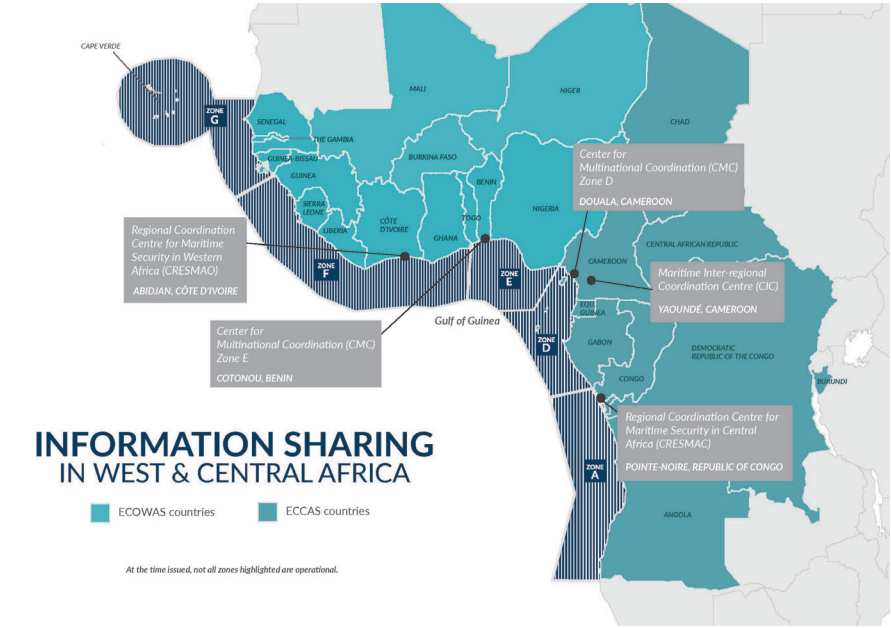
- Information about dangers to the security of navigation. This information, when used alongside official navigational charts, can help to ensure the safety of ships, crew and cargo.
- General security advice, self-protective measures, security procedures and regional contacts, as well as routeing and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

Yaoundé Code of Conduct (CoC)

The Yaoundé CoC is an agreement between nations from West and Central Africa with an intention to cooperate to the fullest possible extent in the repression of transnational organised crime in the maritime domain, maritime terrorism, Illegal, Unreported and Unregulated (IUU) fishing, and other illegal activities.

Yaoundé Architecture for Maritime Safety & Security Space

The Economic Community, ECCAS, ECOWAS and GGC agreed on a MoU to implement the regional maritime strategy within the Central and African common maritime space. This agreement created a number of Maritime Zones covering the overseen by an Interregional Coordination Centre in Cameroon responsible for cooperation, coordination, pooling, and interoperability of community assets.



Map courtesy of one earth FUTURE

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 are fired.
- An actual boarding, whether successful in gaining control of the ship or not.
- Attempts to overcome the SPM using:
  - — Ladders
  - — Grappling hooks or other boarding equipment

Suspicious activity

- The number of crew onboard an approaching skiff 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.
- Skiffs operating far from the coast.
- Vessels fishing outside of normal fishing zones.
- Windows of vessel covered or blanked out.
- Skiffs rafted up.
- No lights during hours of darkness.
- Skiffs with two or more outboard motors.
- Skiffs stopped in the water, no evidence of fishing.

- 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, contact MDAT-GoG & REPORT!

Annex D

MDAT-GoG reporting forms

MDAT-GoG vessel position reporting forms

Once a ship has transmitted an initial report on entering the VRA, MDAT-GoG will request daily reports be transmitted. Upon reaching port/anchorage or upon exiting the VRA, MDAT-GoG will request a final report. The following forms are provided below and can be requested by email to **watchkeepers@mdat-gog.org**

- Initial report.
- Daily report.
- Final report.
- Suspicious/irregular activity report.
- Follow Up Report.

MDAT-GoG vessel position reporting form – initial report

1	Ship Name
2	Flag
3	Call sign and IMO Number
4	INMARSAT Telephone Number
5	MMSI Number
6	Time
7	Position
8	Course
9	Speed
10	Maximum Speed
11	Freeboard
12	Cargo
13	Destination and estimated time of arrival
14	Name and contact details of the CSO
15	Nationality of Master and crew
16	Will Security Services be used?

MDAT-GoG 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	Date/time leaving VRA if applicable

**Preferred time for transmitting the daily report is 1200UTC.*
**Other important information could be change of destination or ETA etc.*

MDAT-GoG 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 anchorage position when leaving the voluntary reporting area

MDAT-GoG suspicious/irregular activity report

1	Own ship's name
2	Own ship's Call Sign and IMO Number
3	Time of Report in UTC
4	Own ship's Position
5	Own 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.

Threats to Maritime Security in the Gulf of Guinea are complex and often result in harm to seafarers. Masters are encouraged to report any signs of suspicious activity.

Follow-up report to MDAT-GoG and IMB PRC

Following any attack or suspicious activity, it is vital that a detailed report of the event is provided to MDAT-GoG and the IMB. The appropriate and relevant information from an incident will be used to support INTERPOL and regional law enforcement investigations.

General Details

1	Name of Ship:
2	IMO No:
3	Flag:
4	Call Sign:
5	Type of Ship:
6	Tonnages: GRT: NRT: DWT:
7	Owner (Address & Contact Details):
8	Manager (Address & Contact Details):
9	Last Port/Next Port:
10	Cargo Details (Type/Quantity):

Details of Incident

1	Date & Time of Incident: LT UTC
2	Position: Lat: (N/S) Long: (E/W)
3	Nearest Land Mark/Location:
4	Port/Town/Anchorage Area:
5	Country/Nearest Country:
6	Status (Berth/Anchored/Steaming):
7	Own Ship's Speed:
8	Ship's Freeboard During Attack:
9	Weather During Attack (Rain/Fog/Mist/Clear/etc, Wind (Speed and Direction), Sea/Swell Height):
10	Types of Attack (Boarded/Attempted/Other):
11	Consequences for Crew, Ship and Cargo: Any Crew Injured/Killed: Items/Cash Stolen:
12	Area of the Ship Attacked:
13	Last Observed Movements of Suspect Craft:
14	Type of Suspicious vessel (Fishing Vessel, Merchant Vessel):
15	Description of Suspicious vessel (Colour, Name, Distinguishing Features):
16	Course and Speed of Suspicious vessel when sighted:

Details of Attackers (if applicable)

17	Number of Attackers:
18	Dress/Physical Appearance:
19	Language Spoken:
20	Weapons Used:
21	Distinctive Details:
22	Craft Used:
23	Method of Approach:
24	Duration of Attack:
25	Aggressive/Violent:

Further Details

1	Action Taken by Master and Crew and its effectiveness:
2	Was Incident Reported to the Coastal Authority? If so to whom?
3	Preferred Communications with Reporting Ship: Appropriate Coast Radio Station/HF/MF/VHF/INMARSAT IDS (Plus Ocean Region Code)/ MMSI
4	Action Taken by the Authorities:
5	Number of Crew/Nationality:
6	Please Attach with this Report – A Brief Description/Full Report/Master – Crew Statement of the Attack/Photographs taken if any.
7	Details of Ship Protection Measures.

Annex E

Other maritime security threats

Illegal, Unreported and Unregulated Fishing

IUU fishing is a significant problem in West Africa. Illegal catches have a detrimental effect on economic development and fish stocks. IUU threatens to contaminate the supply chain and potentially prevent the legitimate export of products to the international market.

IUU fishing in the VRA involves extensive use of fraudulently issued licenses, as well as blatant unlicensed fishing and illegal trans-shipping between purse seiners and reefers at sea.

It is important for the mariner to understand how the fishing vessels that have been involved in criminal activity directly affect seafarers on other vessels. Fishing vessels have, on a number of occasions, been used to facilitate attacks on other vessels. It is also recognised that fishing vessels are occasionally used in smuggling activities and have been involved in the receipt of stolen bunker fuel by at sea STS.

For mariners to understand what suspicious fishing vessel activity is, it is important to be familiar with normal fishing activity. More information on normal fishing activity is available on the MDAT-GoG website.

Trafficking in narcotics

Trafficking of narcotics refers to the global illicit trade of illegal drugs. Maritime routes through the waters off Africa's western seaboard are used as a staging post to traffic cocaine and heroin between the sites of production to the main consumer markets. West Africa is regarded as an important waypoint for traffickers because of inconsistent law enforcement and the increasing production of illegal drugs within the region itself.

Narcotics transiting the VRA are often transported without the knowledge of the ship's owner, operator or Master on internationally trading vessels, in sealed containers that are supposed to be carrying legitimate cargo. Container vessels may unknowingly transport cocaine from producers in South America to Western and Southern Africa, from there it is transported to consumers in Europe. Recent seizures of heroin at port and at sea in West Africa are indicative of the growing use of maritime trafficking routes between production sites in Central and South-East Asia and markets in North America. While transshipment of some narcotics has been reduced by successful intervention and legal action, the movement of large quantities of cocaine gives authorities cause for concern with an increase in quantities seized from shipping containers in West Africa.

Illegal drugs are also moved by much smaller vessels for transshipment or cross decking to other craft for onward conveyance.

The responsibility to disrupt drug trafficking operations in West Africa rests with law enforcement in the region. The shipping industry can support interdiction efforts by remaining alert to and reporting suspicious activity to the MDAT-GoG who are able to inform the appropriate authorities.

Human smuggling, trafficking and Stowaways

The smuggling and trafficking of persons are distinct crimes, but closely linked. Human or migrant smuggling involves the illegal movement of willing and thus complicit persons over an international border. Trafficking of persons does not necessarily involve the crossing of an international border and, unlike human smuggling, involves an element of force, coercion or fraud; people being trafficked are the victims, rather than complicit in the crime. Should a person be smuggled into a country they can become a victim of trafficking through subsequent exploitation.

The trafficking or smuggling of illegal migrants along maritime routes often involves the use of unsafe and crowded vessels, which drastically increases the risk of an incident at sea. Guidance from the IMO is that the shipping industry should be ready to provide all possible assistance to persons in distress at sea, so that they can be rescued and receive fair treatment once safely ashore. This principle is enshrined in international law.

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

- 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 MDAT-GoG for the whole period of activity off the West Coast of Africa. 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 MDAT-GoG 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 (MDAT-GoG, CRESMAC and CRESMAO) 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 MDAT-GoG throughout any voyage.

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

Annex H

Definitions and abbreviations

Definitions

The following terms/definitions to categorise attacks and suspicious incidents that are reported from shipping inside the VRA may be useful and 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.

Hijack A hijack is where attackers have boarded and taken control of a ship against the crew's will. Hijackers will not always have the same motive (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.

Maritime Safety Zone A safety zone is an area extending out from any part of an offshore oil and gas installation (typically 500m) and is established automatically around all installations which project above the sea at any state of the tide. These safety zones are 500m radius from a central point.

Piracy This 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 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.

UNCLOS 60.5

The breadth of the safety zones shall be determined by the coastal State, taking into account applicable international standards. Such zones shall be designed to ensure that they are reasonably related to the nature and function of the artificial islands, installations or structures, and shall not exceed a distance of 500 metres around them, measured from each point of their outer edge, except as authorized by generally accepted international standards or as recommended by the competent international organization. Due notice shall be given of the extent of safety zones.

UNCLOS 101

Piracy consists of any of the following acts:

(a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed: (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft; (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;

(b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;

(c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).

Abbreviations

AIS	Automatic Identification System
CRESMAC	Maritime Security Regional Coordination Centre for Central Africa (Pointe Noire)
CRESMAO	Maritime Security Regional Coordination Centre for Western Africa (Abidjan)
CSO	Company Security Officer
DSC	Digital Selective Calling
DSV	Diving Support Vessel

EEZ	Exclusive Economic Zone
FPSO	Floating Production Storage & Offloading
FSO	Floating Storage & Offloading
GCC	Gulf of Guinea Commission
GoG	Gulf of Guinea
ICC	Interregional Coordination Centre
IMB	International Maritime Bureau
IMO	International Maritime Organization
JWC	Joint War Committee
MSC	Maritime Safety Committee
MDAT-GoG	Maritime Domain Awareness for Trade – Gulf of Guinea
MODU	Mobile Offshore Drilling Unit
MOU	Mobile Offshore Unit
PAG	Pirate Action Group
PCASP	Privately Contracted Armed Security Personnel
PMSC	Private Maritime Security Company
ROV	Remotely operated underwater vehicle
RUF	Rules for the Use of Force
SPM	Ship Protection Measures
SAA	Secure Anchorage Area
SEV	Security Escort Vessel
SSA	Ship Security Assessment
SSAS	Ship Security Alert System
SSO	Ship Security Officer
SSP	Ship Security Plan
UNCLOS	United Nations Convention on the Law of the Sea
VDR	Vessel Data Recorder
VHP	Vessel Hardening Plan
VMS	Vessel Monitoring System
VPD	Vessel Protection Detachment
VRA	Voluntary Reporting Area

Annex I

Supporting organisations

BMP WA 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. Its 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 its 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 are 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

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 organisation's mission is to be the unified global organisation that helps its members succeed by advocating, educating and promoting for the common interests of the cruise community.

www.cruising.org

ICS

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 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. It has 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)** is representing the interests of quality dry cargo shipowners. INTERCARGO convened for the first time in 1980 in London and has been participating with consultative status at the IMO since 1993.

INTERCARGO provides the forum where 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. The Association takes forward its Members' positions to the IMO, as well as to other shipping and international industry fora, having free and fair competition as a principle.

INTERCARGO is committed to safety and quality in ship operations, with a focus on operational efficiency and the protection of the marine environment.

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

IMEC

The **International Maritime Employers' Council Ltd (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 CBAs, 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

ITF

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 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. It is a membership organisation with ship owners, unions and welfare organisation as members. ISWAN works with a range of bodies including PandI Clubs, shipping companies, ports, and governments. Its focus is the wellbeing of the 1.5 million seafarers around the world.

ISWAN supports seafarers and their families who are affected by piracy and its 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 its 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. The Mission to Seafarers runs 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 with an interest in the shipment and terminalling of crude oil, oil products, petrochemicals and gas. OCIMF focuses exclusively on preventing harm to people and the environment by promoting best practice in the design, construction and operation of tankers, barges and offshore vessels and their interfaces with terminals.

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.

Its 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 IMO, to better promote the safety and integrity of gas transportation and storage schemes.

www.sigtto.org

WSC

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 organisation at the IMO.

www.worldshipping.org

Naval/military/governmental organisations

CISMAR

CISMAR is the Integrated Maritime Security Center of Brazil. It aims to contribute to the safety of maritime traffic of interest to Brazil, meet commitments related to Naval Control of Maritime Traffic and the Naval Doctrine Cooperation and Guidance for Shipping assumed by the country, in addition to increasing maritime situational awareness.

Contact:
Email: **cismar-secom@marinha.mil.br**
Telephone: +55 21 2104 6353/6337
Website: **https://www.marinha.mil.br/cismar/**

IFC

The **Information Fusion Centre (IFC)**, based in Singapore, serves as the regional Maritime Security (MARSEC) information-sharing hub covering most of the Indo-Pacific region. With an integrated team comprising International Liaison Officers (ILOs) from more than 19 navies and coast guard; and personnel from the Republic of Singapore Navy (RSN), the IFC facilitates MARSEC information sharing and collaboration between its partners to cue operational responses. Its linkages with more than 90 Operational Centres (OPCENs) from navies, enforcement and maritime agencies in more than 40 countries, as well as linkages with the shipping industry, provide IFC with maritime situational awareness and enables collaboration beyond its Area of Interest.

The IFC collates and analyses MARSEC information to produce accurate, timely and actionable products, which enables 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.

Contacts
Email: **ifc_do@defence.gov.sg**
Telephone: +65 9626 8965 (hotline), +65 6594 5728 (office)
Website: **https://www.ifc.org.sg**

IMB PRC

Established in 1992, the **IMB Piracy Reporting Centre (IMB PRC)** is an independent, non-governmental and not-for-profit organisation which provides the shipping industry with a free 24-hour service to report any piracy or armed robbery attack occurring anywhere in the world.

As a trusted point of contact for shipmasters and ship owners, all reported attacks are immediately relayed to the most relevant government response agency seeking their support to render assistance to the ship in distress. Inmarsat Safetynet broadcasts to ships and alerts to CSOs via email are also sent out which help alert other seafarers and save lives at sea.

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

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 three days of a hijacking of their ship.

MDAT-GoG

Maritime Domain Awareness for Trade – Gulf of Guinea (MDAT-GoG) is a cooperation centre between the Royal Navy (UKMTO) and the French Navy (MICA-Center) in support of the Yaoundé Process. This centre has been in operation since June 2016. The primary output from the MDAT-GoG is to contribute by maintaining coherent maritime situational awareness in the central and western African Maritime areas, with the ability to inform and support industry. It contributes to the safety and security of the Mariner in the regional maritime domain.

NIMASA

The **Nigerian Maritime Administration and Safety Agency (NIMASA)** is committed to the enthronement of global best practices in the provision of maritime services in Nigeria. Our areas of focus include effective Maritime Safety Administration, Maritime Labour Regulation, Marine Pollution Prevention and Control, Search and Rescue, Cabotage enforcement, Shipping Development and Ship Registration, Training and Certification of Seafarers, and Maritime Capacity Development. Using modern tools that guarantee efficiency and effectiveness, we are determined to develop indigenous capacity and eliminate all hindrance.

ICC-Gulf of Guinea-Yaoundé

The **Interregional Coordination Centre (ICC)** is the coordination and information-sharing structure which connects the Regional Maritime Security Centre for Central Africa (**CRESMAC**) and the Regional Maritime Security Centre for Western Africa (**CRESMAO**).

MDAT-GoG
+33 298 228888