# BMP MARITIME SECURITY



# Produced and supported by:






















































































































# Version control

| Edition | Published date | Change |
|---|---|---|
| First | March 2025 | |
| First | June 2026 | Section 6 Incident response: new content on actions on boarding by activists |

# BMP Maritime Security



**Legal notice**
BMP Maritime Security (BMP MS) has been developed purely as guidance to be used at the user's own risk. No responsibility is accepted by the authors, their members or by any person, firm, corporation or organisation for the accuracy of any information in BMP MS or any omission from BMP MS or for any consequence whatsoever resulting directly or indirectly from applying or relying upon guidance contained in BMP MS even if caused by a failure to exercise reasonable care.

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

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

**Exceptions:**
The permission does not extend to using the photographs separately outside of BMP MS as these photographs belong to a third party. Authorisation to use the photographs separately from BMP MS must first be obtained from the copyright holders, details of whom may be obtained from the authors.

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

BMP Maritime Security replaces any existing global or regional guidance issued or supported by the signatories.

Background and supporting information are available at: www.maritimeglobalsecurity.org

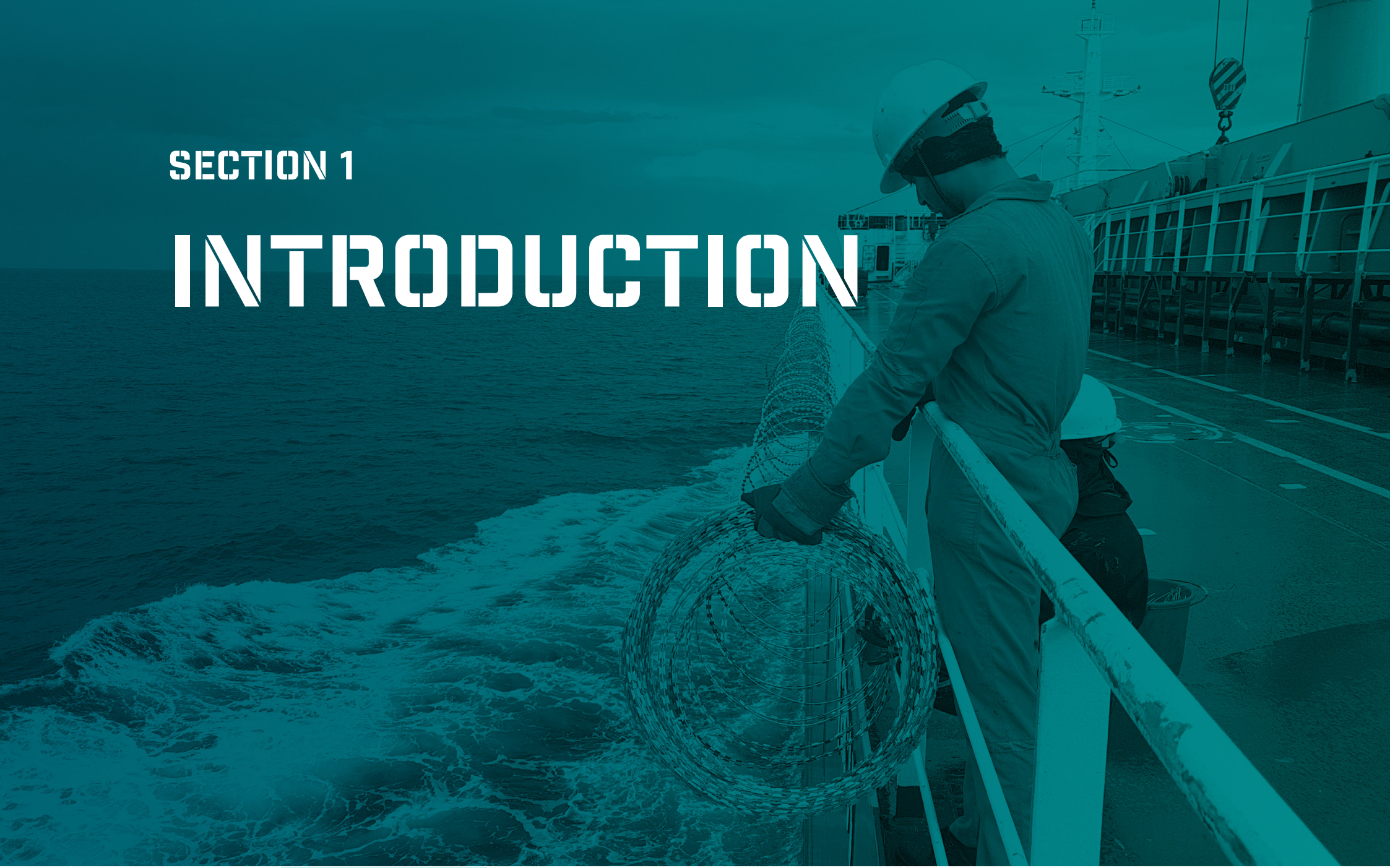
Design: Phil McAllister Design

# CONTENTS


| | | |
|---|---|---|
| 1 | Introduction | 06 |
| 2 | Maritime security threats | 10 |
| 3 | Threat and risk assessment | 16 |
| 4 | Planning | 21 |
| 5 | Mitigation measures | 25 |
| 6 | Incident response | 37 |
| 7 | Post-incident procedures | 43 |
| Annex A | Reporting and information centres | 46 |
| Annex B | Seafarer welfare support | 55 |
| Annex C | Maritime lexicon and abbreviations | 57 |

SECTION 1

# INTRODUCTION



# Introduction to Best Management Practices Maritime Security

Best Management Practices (BMP) Maritime Security (MS) consolidates previously published regional BMP documents into a single, comprehensive publication. It focuses on a threat and risk management process addressing globally applicable threats and mitigations, as well as providing references to external sources for up to date regional information.

Seafarers operating ships around the world encounter various maritime security threats, state and non-state. These threats often involve aggressive attackers who subject persons to violence and ill-treatment, hijack ships for ransom or cargo theft, and, in some cases, hold seafarers as hostages for extended periods. Attackers' motivations may be criminal, ideological or political, and attacks may be targeted or opportunistic. Maritime security threats vary across regions and within them both in terms of the threats themselves and their severity.

The purpose of this publication is to help all ships plan their voyage and to detect, avoid, deter, delay and report attacks and incidents wherever they may occur. Experience has shown that following the recommendations BMP offers makes a significant difference to the safety of seafarers.

## Benefits of implementing BMP

Applying these recommendations will:

- Assist in planning voyages and offshore activities.
- Improve understanding of maritime threats and their impacts.
- Reduce the likelihood of being involved in a maritime security incident.
- Help in determining mitigations to keep the crew and ship safe.
- Provide reference information sources.
- Specify contacts and reporting procedures for emergencies and welfare assistance.

## Applicability and guidance

- **BMP measures:** not all mitigation measures are applicable to every threat, ship type or region.
- **Usage:** companies, Company Security Officers (CSOs), Ship Security Officers (SSOs), and Masters should use this guidance to conduct ship specific threat and risk assessments aimed at protecting seafarers, ships, and cargo. BMP is also a useful reference for charterers and other maritime stakeholders.
- **Complementary guidance:** this guidance complements other industry guidelines and international recommendations, including IMO, Flag State and P&I Circulars.
- **BMP** complements but does not override International Ship and Port Facility Security (ISPS) Code requirements.

## Additional resources

- Online resources: access further information and links at Maritime Global Security.

**ATTENTION**

**Master's Authority**
**This guidance does not override the Master's overriding authority and responsibility to protect the crew, ship, and cargo.**

## Using this guidance

This Best Management Practice (BMP) is designed to support a structured approach to threat and risk assessment in the maritime environment. It offers the reader guidance on the following areas:

1. **Understanding maritime security threats:** insights on known threats and where to access additional information.
2. **Threat and risk assessment:** methods for identifying and evaluating threats and risks.
3. **Planning:** steps to consider when planning a voyage or offshore activity.
4. **Mitigation:** measures to reduce or eliminate identified risks.
5. **Incident response:** actions to take in the event of a security incident.
6. **Post-incident considerations:** steps to follow an incident, including recovery and analysis.
7. **Global reporting and information centers:** resources for reporting incidents and obtaining real-time information.
8. **Seafarer welfare support:** aiding the well-being of crew members by outlining support available to them.

BMP is arranged in a structured manner, with a navigation toolbar at the bottom of each page that allows readers to easily move through the document and access key references. As security threats in the maritime domain are constantly evolving, external signposts are included to guide the reader to sources for up-to-date information and data.

Users are encouraged to seek a comprehensive understanding of the maritime environment, and the security risks that may be faced. This includes using all available resources as part of the ongoing threat and risk assessment process.

## Conclusion

By following the BMP, both companies and seafarers can minimise the risk of maritime security incidents, ensuring better protection against emerging threats and improving overall safety.

**USERS ARE ENCOURAGED TO SEEK A COMPREHENSIVE UNDERSTANDING OF THE MARITIME ENVIRONMENT, AND THE SECURITY RISKS THAT MAY BE FACED**

## The fundamental requirements of BMP

### 1. Understanding the threat

- **Dynamic nature:** maritime threats are constantly evolving.
- **Current information:** obtaining up-to-date information is crucial for effective threat and risk assessment and decision-making.

### 2. Conducting risk assessments

- **Assessment:** companies must conduct thorough threat and risk assessments.
- **Ship mitigations:** identify and implement measures to protect the crew and ship.
- **Crew training:** ensure the crew is well-briefed and trained.
- **Situational awareness:** know your operating environment.
- **Guidance:** comply with Flag State requirements, industry guidance and implement military recommendations where appropriate.

### 3. Reporting

- **Voluntary registration and reporting:** register and report to regional centres as appropriate.
- **Incident reporting:** report incidents and suspicious activities to recognised reporting centres and the Flag State Administration.
- **Distress signals:** send distress signals when under attack.



### 4. Cooperation

- **Shipping and military forces:** cooperate with other ships and military forces as necessary.
- **Law enforcement:** work with relevant law enforcement and authorities to preserve evidence.
- **Welfare providers:** collaborate with welfare providers to provide psychological and/or logistical support (annex B).

**COLLABORATE WITH WELFARE PROVIDERS TO PROVIDE PSYCHOLOGICAL AND/OR LOGISTICAL SUPPORT**

SECTION 2

# MARITIME SECURITY THREATS



# Maritime security threats

Maritime security threats can be broadly categorised into physical and virtual threats.

## Physical security threats

Physical threats to maritime security can originate from the air, land or sea and are generally easier to identify compared to virtual threats. These threats can include:

- **Physical attacks:** ships may come under attack from various weapons launched from aircraft (including helicopters), ships, submarines and land-based sites. These weapons have included bombs, rockets, machine guns, Water-Borne Improvised Explosive Devices (WBIEDs), one way attack drones and missiles. In addition to one way attack drones, Unmanned Aerial Vehicles (UAVs) and Uncrewed Surface Vehicles (USVs) may also be used for surveillance and to support loitering munitions in conducting attacks.
- **Seizure:** ships have been illegally seized and held for prolonged periods by state and non-state actors.
- **Piracy:** pirates use various boat configurations, including small high-speed skiffs and motherships, which allow them to operate over larger areas. They typically use small arms and Rocket Propelled Grenades (RPGs) to intimidate shipmasters and attempt to board the ship using ladders or ropes. Successful boardings are more likely at night.
- **Illegal boardings:** in addition to piracy boardings using ladders and hooks, more aggressive boardings have been seen involving fast attack boats and helicopters to land or fast-rope forces onto a deck.
- **Criminal activity:** illegal boarding with intent to steal shipboard equipment or seafarers' possessions, money, etc, is commonplace in some ports. Such attackers can be armed, most usually with bladed weapons, and can present a physical threat to crews. Such threats usually, but not exclusively, occur in traffic separation schemes where dense traffic exists, and territorial waters, particularly ports and anchorages. Illegal boardings may also occur while a ship is underway. In many cases, the intent is to steal, rather than taking control of the ship.



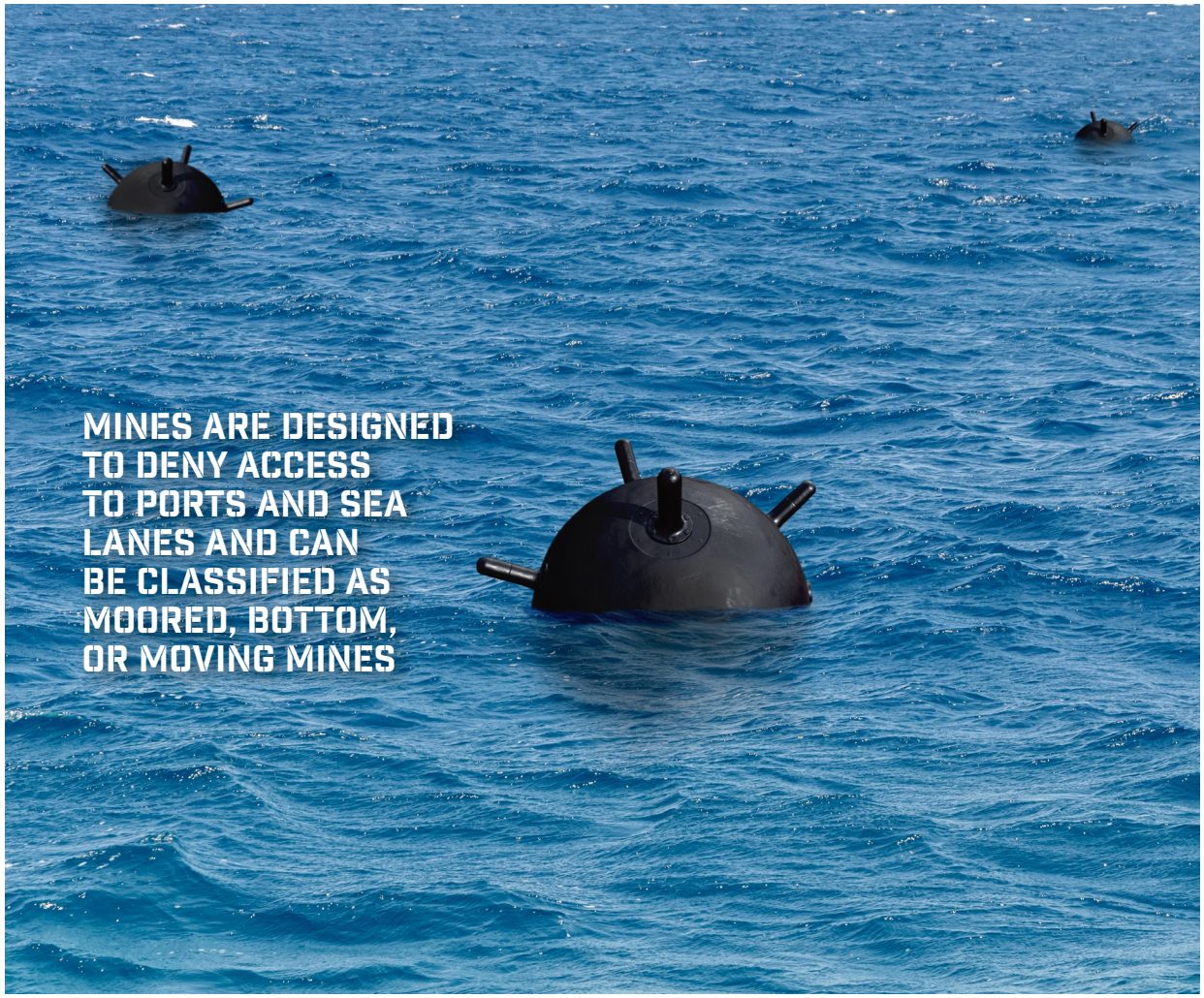
**Typical pirate skiff**

## Specific threats

- **Water-Borne Improvised Explosive Devices (WBIEDs):** These have been used against merchant ships in conflict regions. WBIEDs can be crewed or uncrewed surface vessels. Incidents have occurred where a WBIED has been controlled from a distance or from an accompanying mothership or operates autonomously. Mitigation measures to prevent contact with the ship's hull are limited. Masters should recognise the intent of these attacks is to cause damage and not necessarily to board the ship.

- **Sea mines:** a sea mine is an explosive device laid in the water with the intention of damaging or sinking ships or of deterring shipping from entering an area. The term does not include devices attached to the bottom of ships or to harbour installations by personnel operating underwater, nor devices which explode immediately on expiration of a predetermined time after laying. Mines are designed to deny access to ports and sea lanes and can be classified as moored, bottom, or moving mines.

a. Moored mines (also known as buoyant mines): a mine of positive buoyancy held below the surface by a mooring attached to a sinker on the seabed. Its firing system can be of either contact or influence type. Some 'deep moored



mines' use extremely strong moorings (usually small gauge wire) to permit use in water depth down to 1,000 metres. If the mooring cable breaks, then the moored mine becomes a moving (floating) mine.

b. **Bottom/ground mines:** bottom/ground mines are negatively buoyant devices that rest on, or can become buried in, the seabed and are held there by their own mass. The firing system is usually of the influence type. They can be triggered by any influence (acoustic, magnetic, seismic, pressure), or a combination of these influences. These types can be laid up to maximum water depths of 120m, depending on the target and/or the amount of explosive charge, but water depths up to 60m are more suitable.

c. **Moving mines:** this is a collective description of mine types that are not stationary. All floating, oscillating, rising or homing mines belong to this category. As an example, rising mines can be laid at a depth of 500m (mine case) and 2,400m (anchor).

d. **Limpet mines:** these are commonly manually attached by a swimmer or diver on the underside of a ship's hull, usually with magnets. Unlike larger mines, limpet mines are not intended to sink a ship but immobilise it.

If there is intelligence suggesting the presence of sea mines in an area, visual sightings, or a confirmed explosion from a sea mine, then a Mine Threat Area (MTA) or a Mine Danger Area (MDA) would be established and broadcast to maritime traffic via navigational area (NAVAREA) warnings.



**ANTI-SHIP MISSILES (ASM) ARE LONG RANGE, ACCURATE AND POWERFUL WEAPONS AND HAVE BEEN USED AGAINST MERCHANT SHIPS IN THE RED SEA**

- **Anti-Ship Missiles**
  Anti-Ship Missiles (ASM) are long range, accurate and powerful weapons and have been used against merchant ships in the Red Sea. Other ships may be hit if the missile controller targets the wrong ship or the missile homes in on an unintended target. They pose a significant threat due to their destructive power causing fatalities and catastrophic damage.

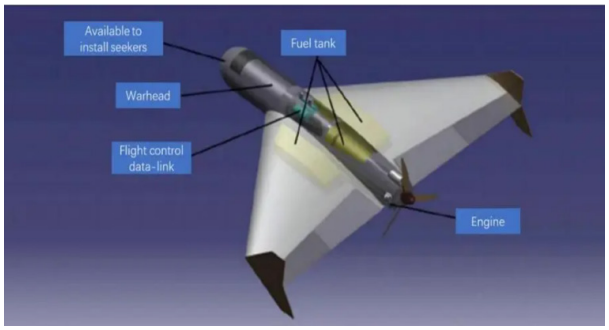
  ASMs can be launched from a variety of ships, submarines and aircraft as well as from land. They can be launched from short range to hundreds of miles. These missiles can be of a cruise or ballistic nature:
  - Cruise missiles are jet-propelled and travel at subsonic speeds. Their sensors are very accurate.
  - Ballistic missiles are rocket-powered to get into flight, after which they follow an arching trajectory to the target.

  The launch of an ASM may be detected through a visible flash and smoke. Missiles will normally hit above the waterline. The main hazard is likely to come from fire, caused either by the warhead explosion or by the unspent fuel from the missile motor.

Missiles can be fired in a straight line or follow a predetermined course to a target or dead reckoning (DR) position. They can have an active or passive seeker head using optical, electronic or heat signature homing to locate targets.

- **Loitering Munitions**
  Loitering Munitions (LM) are a form of UAV with a built-in weapon and the capability to loiter (wait passively) in the target area until the target is located. The number of LM attacks against both civilian and military ships, especially in the Red Sea and Middle East, has risen. The global proliferation of these rapidly advancing autonomous technologies, to both state and private actors, poses a significant security threat to commercial shipping.

  More information regarding the threat from LM can be found here.




## Virtual security threats

Virtual threats primarily involve cyber-attacks on electronic systems, which can impact ship navigational systems, disrupt Global Navigation Satellite System (GNSS) or spoof Automatic Identification System (AIS) services. These threats are harder to detect and require comprehensive procedures such as:

- Backup systems and processes.
- Situational awareness training.

General guidance for cyber security onboard ships can be found at www.maritimeglobalsecurity.org

**ATTENTION**

**Navigators should use all available methods and not rely on GNSS alone.**

## Regional maritime threats

Maritime security threats vary globally and within geographical regions. A variety of threats may be present in any one area at varying intensities depending on the intent and capability of attackers. Recognising this, reporting centres and industry associations produce information on regional threat actors, their intent and capability to attack merchant shipping, and link these to applicable BMP measures to mitigate the threat. The industry website is at www.maritimeglobalsecurity.org and a list of global reporting centres at annex A.

To mitigate these threats, continuous improvement through regular security drills and exercises, capturing lessons observed, and adapting to new technologies is essential. Merchant ships should maintain close coordination with military forces and leverage commercial intelligence and open-source services for threat updates.

## Specific virtual threats

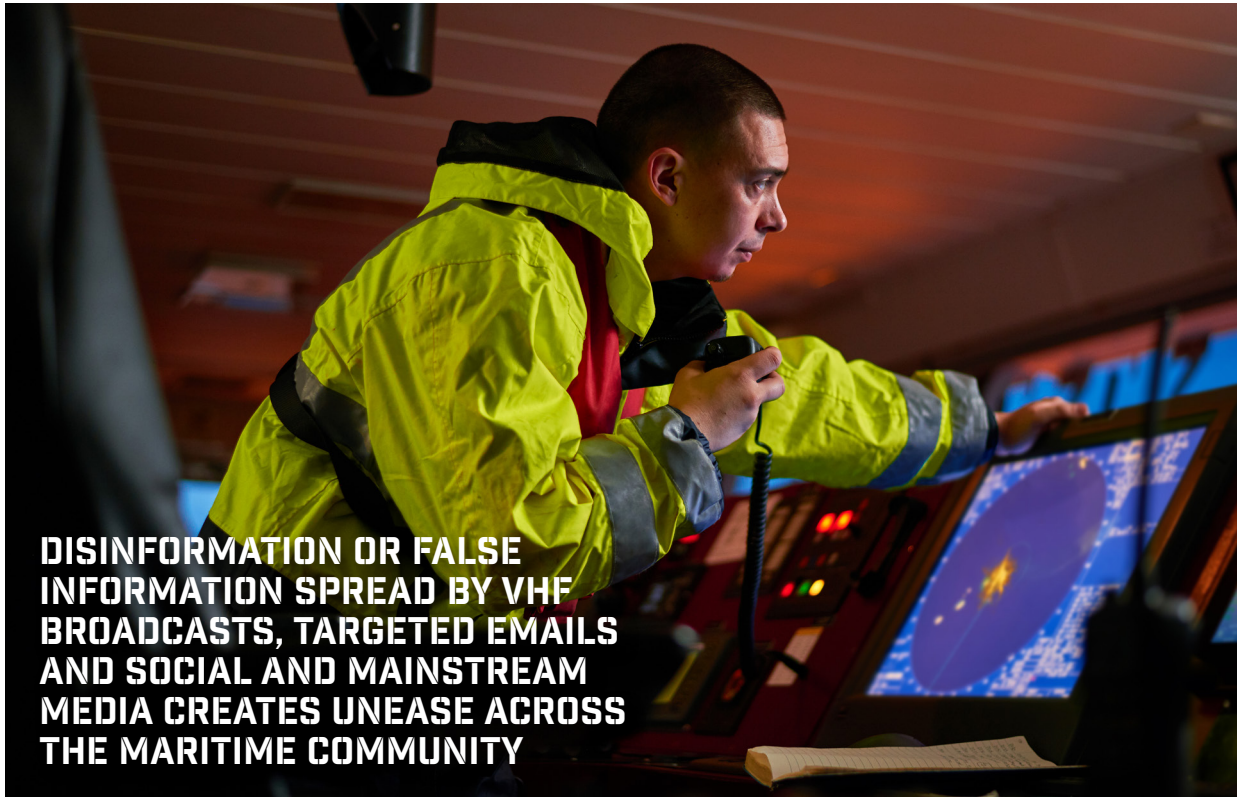
### GNSS jamming and spoofing

Jamming disrupts GNSS signals, while spoofing provides false signals to deceive navigation systems.

a. **Jamming** is usually caused by interference to the signals at GNSS frequencies. Intentional jamming is designed to overpower the very weak GNSS signals received. Experience has shown military jammers have a disabling effect in areas of conflict.

b. **Spoofing** is the provision of like signals, transmitted locally and coded to fool a receiver to think it is somewhere it is not. A GNSS spoofing attack attempts to deceive a GNSS receiver by broadcasting incorrect GNSS signals. These spoofed signals may be modified in such a way as to cause the receiver to estimate its position to be somewhere other than where it is, or to be located where it is but at a different time, as determined by the attacker.

c. Deliberate **AIS spoofing** occurs when a ship transmits incorrect AIS data. The AIS data is manipulated to show the ship in one location when in fact it is operating in another. Fake AIS signals have been observed for ships that appear on navigational systems but do not exist.




Navigators should compare all electronic data, and especially AIS, with other information sources to detect spoofing attempts.

### Disinformation

Disinformation or false information spread by VHF broadcasts, targeted emails and social and mainstream media creates unease across the maritime community. False threats indicating ships will be targeted cause crew anguish. Third parties may impersonate authorities to obtain information from the ship. Care should be taken to verify all statements received with the appropriate authorities.




SECTION 3

# THREAT AND RISK ASSESSMENT

# Threat and risk assessment

The threat and risk assessment forms the foundation for ship mitigations and layered defence strategies. This section provides an overview of threat and risk assessments, while hardening measures are detailed in section 5. The process starts with a threat assessment and works through each subsequent layer towards ship control and safety.




A threat assessment should cover all security threats relevant to the voyage or offshore activity. It is crucial to incorporate the latest threat advice in every threat assessment before a voyage or offshore activity. Refer to annex A and industry website www.maritimeglobalsecurity.org for security threat information and source references.



## Components of a threat

A threat is composed of three elements: capability, intent, and opportunity.




- **Capability:** the physical means attackers possess to conduct an attack.
- **Intent:** the demonstrated willingness to carry out attacks.
- **Opportunity:** the aspect that can be mitigated by the company, charterer, ship and crew through the application of security measures.

While companies and ships' Masters cannot influence an attacker's capability or intent, they can minimise the opportunity for attacks. Supplemental information about threat characteristics, specific or new tactics and regional background factors can be obtained from global reporting centres and organisations listed in annex A. Removing any one side of the threat triangle minimises the threat.

## Determining the threat

All available information sources should be considered to determine the threat and may include but are not limited to:

- **Flag State:** guidance and advisories provided by governments and national authorities.
- **Industry information:** the industry maritime security website, www.maritimeglobalsecurity.org provides guidance on a range of security issues. The website is regularly reviewed and updated to reflect operational and industry feedback or to address significant security incidents.
- **Maritime Security Bulletins:** updates on security-related incidents and risks.
- **Regional coordination and information sharing:** regional maritime coordination and information-sharing centres provide area-specific guidance. These centres should be consulted during the initial stages of threat and risk assessments or voyage preparation to ensure a comprehensive understanding of local risks.
- UKHO Security Charts: detailed regional security guidance (refer to annex A for further details).
- **Military information:** intelligence and advisories from military organisations.
- **Military contributions:** in specific areas, militaries provide additional threat information. For example, in the Middle East:
  - The Joint Maritime Information Centre (JMIC) offers incident analysis.
  - EUNAVFOR and CMF produce Industry Releasable Threat Assessments (IRTAs) and Industry Releasable Threat Bulletins (IRTBs) to aid risk management.
  - UKMTO issues warnings and advisories. A list of all authorities offering maritime security advice is provided in annex A.
- **Commercial intelligence services:** threat analysis and risk insights from private sector providers.
- **Open-source material:** relevant publicly available security threat information.




Risk assessment is a critical component of voyage planning and offshore activity within a safety management system and Ship Security Plan (SSP).

The risk assessment should note the identified threats, evaluate the risks, and determine the measures for prevention, mitigation and recovery.

The risk assessment should consider the following:

- Who or what might be harmed and how?
- What is the severity and frequency?
- What is already in place to control the risks?
- What further action is needed to control the identified risks?
- Who needs to implement the actions?




When assessing risk, the following should be considered:

- Requirements of the Flag State, company, charterers and insurers.
- The ship's characteristics, vulnerabilities, and inherent capabilities, including citadel/safe muster points and secondary muster points (freeboard, speed, general arrangement, etc.).
- The ship's and company's standard operating procedures (drills, watch rosters, chain of command, decision-making processes, etc.).
- Background factors such as owner/operator affiliations, traffic patterns and local patterns of life, including fishing vessel activity.
- Impact on crewing of International Bargaining Forum (IBF) warlike operations areas.
- Cooperation with military authorities should be considered, but mitigations should not be based on the availability of naval assets unless direct military support has been agreed.
- The use of Private Maritime Security Companies (PMSC).
- The use of Security Escort Vessels (SEV).

Regular review of the Ship Security Assessment (SSA) and voyage risk assessment is recommended to ensure:

- New threats are identified, and existing risks are confirmed or removed.
- Mitigations remain robust, practical and realistic.
- Post-incident lessons are captured.
- Updates to industry best practice.

A Vessel Hardening Plan (VHP) should be created based on the risk assessment, outlining mitigation measures needed to reduce risk to As Low As Reasonably Practicable (ALARP). The VHP can be a standalone document, part of company procedures, or included in the SSP.

All voyages and offshore activities require thorough advance planning using all available information. Maritime threats are dynamic, making it essential to have a detailed threat and risk assessment for each voyage and activity.

Further guidance on risk assessments and how to develop a VHP can be found at www.maritimeglobalsecurity.org.





SECTION 4

# PLANNING

# Planning

## Company planning

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 to mitigate against the risk of attack. It should be noted that risks will vary across regions.



The following should be considered by companies when planning:

1. Regular review of threat and risk assessments
   - Continuously update plans based on the latest threat and risk assessments.
2. Security documentation
   - Review Flag State requirements, SSP, VHP, company mandated mitigation measures and local military advice.
3. Insurance and liabilities
   - Consider possible additional insurance and other commercial liabilities that may be necessary when transiting threat areas.
4. Guidance to the Master
   - Prepare recommended route, updated plans, and requirements for group transits and national convoys.
5. Due diligence of PMSCs
   - Before contracting PMSCs proper due diligence should be exercised, for example by selecting PMSCs holding valid certification against relevant ISO standards such as ISO 28007 or ISO 18788.
6. Review crewing requirements
   - Review and adjust personnel requirements; consider additional personnel for security duties or disembarking non-essential persons.
7. Guidance and crew training for security threats
   - Provide guidance, training and exercises for the crew on identifying and reacting to security threats. Support for seafarers' wellbeing should always be considered, especially if an incident has occurred.
8. Placement of hidden position transmitting devices
   - Consider installing hidden position transmitting devices to locate the ship if usual transmitting devices are disabled.

## General

### Information security

To prevent critical voyage information from falling into the wrong hands:

1. Minimise external communications
   - Limit communications with external parties, relating to the coordination of rendezvous points or waiting positions.

2. Control email correspondence
   - Control email content to agents, charterers and chandlers, ensuring it is concise and contains only the minimum required information.

3. Data hygiene
   - Minimise electronic transmissions and data transmitted from the ship, including social media.

4. Social media
   - Seafarers should be aware of the impact of sharing images of an attack on social media channels or any form of communications. The internet and social media channels should be used responsibly.



**ATTENTION**

**Never share the ship's location or route on personal social media channels.**

### Tracking/monitoring and reporting

Attackers may have used communication systems like AIS to target specific ships. To mitigate this risk, companies should consider implementing independent protected fleet tracking systems. Important factors to assess include system redundancy and reliance on existing onboard communication systems.

### Radar:

- Proper placement of radar antennas can minimise blind sectors caused by the superstructure.
- Additional radars and specialist software can enhance the detection of small objects that standard radars might miss.
- Standard S and X Band radar sets may struggle to detect small craft, especially those with hulls made of Glass Reinforced Plastic (GRP) or wood.
- As technology improves, companies could consider installing new equipment or upgrading their current systems.

## Vessel planning

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, to mitigate against the risk of attack.

### Prior to any voyage or offshore activity

1. Obtain the latest threat information from the authorities listed at annex A and the Maritime Global Security website.
2. Review the company risk assessment and if required conduct a specific voyage or activity risk assessment.
3. Check the latest NAVAREA warnings and alerts.
4. Review industry, Flag State, company and military routing advice.
5. Implement registration and reporting requirements as per annex A.
6. Plan equipment availability for vessel hardening.
7. If used, confirm the PCASP embarkation plan and rendezvous arrangements for SEVs.



**ATTENTION**

**If the risks cannot be managed to ALARP, reconsider the voyage or activity.**

### Prior to entering an area of increased threat

1. Implement security measures in accordance with the mitigations described in the risk assessment.
2. Brief the crew and conduct drills:
    - Brief the crew on preparations.
    - Conduct drills with mitigations in place.
    - Review the emergency plan and ensure all crew are aware of their duties.
    - Ensure familiarity with the alarm signals for an attack and an all-clear situation.
    - Check:
        - Essential equipment tested and available.
        - Hardening in place, including the security of all access points.
        - Lockdown conditions, considering crew safety.
        - Bridge team's security knowledge and crew awareness.
        - Crew's response to different threats.
3. Determine reporting requirements as outlined in annex A.

### Other considerations

1. Emergency communication plan:
    - Prepare and test an emergency communication plan with essential contact numbers (see annex A) and prepared messages.
    - Display communication plans near all external communication stations, including the safe muster point and/or the citadel.
    - Test communication devices and the Ship Security Alert System (SSAS).
    - Consider the provision of a 'safe word' held by selected crew for communication authentication with officials.
2. AIS policy:
    - Carefully consider AIS policy in threat areas.
    - Consider the safety and security implications of broadcasting AIS:
    - If AIS is turned off, alter course and speed to minimise tracking by dead reckoning.
    - If AIS is used, restrict data to ship's identity, position, course, speed, navigational status, and safety-related information.
3. Planned maintenance:
    - Reschedule maintenance of voyage-critical equipment for transit through areas of increased threat.
    - Consider cargo management duties to reduce risk of crew working on exposed decks.

### In an area of increased threat

1. Report to centres per annex A and if stipulated in any charter agreement.
2. Monitor the latest threat information.
3. Regular check of all mitigations and especially control of all access points.
4. Identify a safe area for drifting, loitering, anchoring and slow steaming whenever possible.
5. Minimise use of VHF; prefer email or secure satellite phone communications. Only respond to known or legitimate callers on VHF, considering the possibility of imposters.
6. Maintain social media hygiene. Photographs and information on social media can provide details on the ship's location, intent and operations.

### Seafarer wellbeing

Seafarers face unprecedented maritime threats which may affect their welfare and mental wellbeing. Planning should consider crew support such as the provision of a 'welfare ambassador' and regular discussion regarding the helplines and services available to them. Details can be found in annex B.



SECTION 5

# MITIGATION MEASURES

# Mitigation measures

To effectively mitigate against attacks, ship crews should implement well-planned and rehearsed measures as part of a comprehensive Vessel Hardening Plan. This plan should detail the rigging of physical barriers and include regular drills and exercises for the crew to practice responses to various threats.

The guidance provided is informed by global experiences of attacks to date. It is important to note that not all methods will be applicable to every region or ship type. The specific measures adopted should be based on a thorough threat and risk assessment for each ship or offshore activity.

### Key considerations for vessel hardening

1. **Compliance with safety regulations:** any vessel hardening measures must comply with the International Convention for the Safety of Life at Sea (SOLAS) regulations. This means ensuring escape routes remain accessible and the crew's ability to respond to non-security emergencies is not compromised.

2. **Attacks:** ships can be attacked while underway or stationary (e.g., at anchor, during ship-to-ship or single buoy mooring operations, or while drifting). Therefore, vessel hardening measures must be effective in all scenarios.

3. **Layered defence:** implementing a layered defence system increases the complexity for would-be attackers, thus enhancing the ship's security integrity. Each layer adds to the overall resilience and unpredictability of the security measures.

4. **Customising measures:** companies should have detailed guidance on vessel hardening based on their specific risk assessments. They may also consider further alterations to the ship, obtaining additional equipment, or increasing manpower to further reduce the risk of attack.

### Routing

Vessel routing can play a key role in reducing risk. During the risk assessment process, the routing should be considered in view of the following:

- Locations of recent attacks.
- Intelligence reports of threats (e.g. Pirate Action Group activity).
- Sailing in territorial waters.
- Routing through areas where the weather may assist in mitigating the risk.
- Industry routing guidance – Maritime Security Transit Corridors.
- Avoidance of the area.

### Alarms

Ship's alarms serve to inform the crew of an attack and warn the attackers the ship is aware and reacting. Continuous sounding of the ship's whistle may also distract attackers. It is crucial that:

- 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 supplemented by information over the accommodation and deck PA system, relating to the type of attack. This ensures the crew muster at the appropriate location.
- Drills are conducted to ensure the alarm and PA broadcast can be heard throughout the ship, and the crew are familiar in moving to a position of safety.
- All PA systems and speakers are checked regularly to ensure they are in working order.

### Watch keeping and enhanced vigilance

The Master should implement the following actions to enhance 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 the alertness of the lookouts.
- Ensure sufficient binoculars are available for the enhanced bridge team, preferably anti-glare.
- Consider using thermal imagery optics and night vision aids, as these provide 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.
- If applicable, consider placing well-constructed dummies at strategic locations around the ship to give the impression of a larger crew on watch.
- Use CCTV and fixed searchlights for better monitoring; fixed searchlights can deter approaches from the stern.



**ATTENTION**

**A good lookout is one of the most effective methods of ship protection. They can help identify a suspicious approach or attack early, allowing for defences to be deployed.**

### Manoeuvring

Experience has shown evasive or counter action manoeuvres for some vessel types, while avoiding reduction in speed, makes boarding and targeting more difficult.



**WARNING**

**Avoidance manoeuvres should only take place when it is safe to do so.**




### Preventing access at sea primarily involves installing physical barriers.

Physical barriers are designed to make it as difficult as possible for attackers to board the ship by increasing the difficulty of the climb. When planning barrier placement, special consideration should be given to ships with sunken poop decks. Typical physical barriers include:

- Razor wire: also known as barbed tape, it creates an effective barrier if properly rigged and secured. High tensile concertina razor wire with coil diameters of 730mm or 980mm is recommended. Use a double roll or a high-quality single roll outboard of the ship's structure, ensuring it is properly secured to prevent attackers from pulling it off.

- Spikes: these consist of several sharp points attached to a bar and mounted outside the ship's handrails. They can be made of steel or GRP. While effective, they require storage space when not in use and time to rig and de-rig.

- Plastic or GRP barriers: these fit over the ship's rails and make it difficult for ladders or grapples to hook on. They are rigid and usually 'P' shaped in profile. However, they require considerable storage space when not in use and can be damaged in heavy weather.

- Chain link fencing: a double layer of chain link fencing is effective against aggressive tactics such as RPG attacks. It is typically fitted around the outer perimeter of the bridge deck using scaffolding poles and clamps. However, it is time-consuming to rig and de-rig, and clamps can damage the paintwork, causing corrosion. It is not effective if placed close to or against bridge windows.

### Summary of physical barriers

- **Razor wire:** high tensile concertina razor wire is recommended. Secure it properly, use personal protective equipment, and obtain in short sections for easier handling.
- **Spikes:** effective but require storage space and time to rig. Permanently fitted spikes could resolve this issue.
- **Plastic or GRP barriers:** effective but require storage space and can be damaged in heavy weather.
- **Chain link fencing:** effective against aggressive tactics but time-consuming to rig and can cause corrosion. In the event of bad weather, chain link can easily become twisted, unhooked and completely inoperative.



**ATTENTION**

**Security measures to control access must not compromise the crew's ability to abandon the ship or manage other emergencies.**

### Water and foam cannon systems

Water hoses, foam monitors and water cannons can deter or delay intruders trying to board the ship. It is recommended to rig them in fixed positions before entering threat areas, as adjusting them under threat exposes the operator. Installing a fixed baffle plate in front of the water jet nozzle can increase coverage.









### System options:

- **Fire hoses:** deliver a single jet of water and should be secured firmly to the railings.
- **Water cannons:** deliver water in a sweeping arc and can be operated remotely.
- **Spray rails:** create a water curtain over the ship's side and can be operated remotely.
- **Fire monitors:** useful for washing down the side of a ship or across the deck to deter fast-roping from helicopters.

### Considerations:

- Water spray and fire monitors are effective in deterring or delaying illegal boarding attempts.
- Fixed positioning of hoses and fire monitors is recommended for covering likely access routes.
- Use fire hoses in jet mode with baffle plates for improved water coverage.
- Water cannons can protect a larger part of the hull.
- Ensure all available fire and general service pumps are ready for use, possibly requiring additional power.
- Conduct drills to ensure effective coverage of vulnerable areas.

### Ballast overflow

Ballast overflow involves intentionally overflowing ballast tanks to create a large volume of water flowing across the deck and over the ship's side, hampering intruders trying to board. Care should be taken to prevent excessive pressure buildup in any compartment for example, opening the tank lids rather than overflowing through vents.

### Propeller arresters

Propeller arresters are designed to foul the propeller and stop the engine of a small boat, preventing it from coming alongside and boarding. Evaluate the position of the arresters to avoid adverse impacts on the ship. Environmental factors like wind speed and wave height can reduce effectiveness.

### Other physical barriers

Various barriers can prevent illegal boarding:

- **Hanging obstacles:** swinging obstacles over the ship's side.
- **Overhanging protection:** designed to prevent climbing over the ship's rails.
- **Sandbags, water barrels, and steel plating:** especially around vulnerable areas like the bridge.
- **Removable barriers:** around pilot boarding points to avoid de-rigging large areas before port arrival.
- **Steel bars on portholes and windows:** prevent access through these openings.
- **Fixed nets and/or ropes:** strung across the main deck may prevent a helicopter landing or boarding by fast-roping.

**WARNING**

**All systems should be secure before entering the harbour and not interfere with safety operations while recognising that in some areas this may be a vulnerability.**







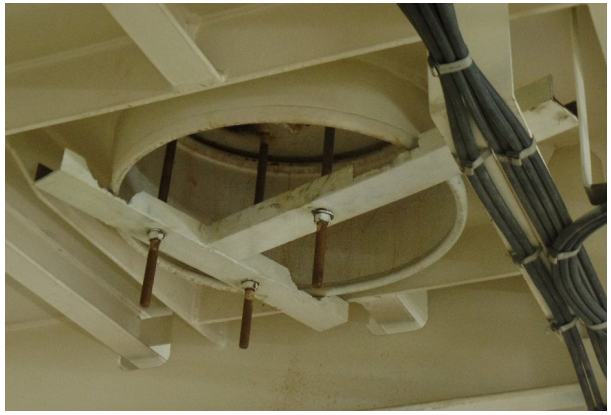

## Measures to prevent or delay access to accommodation blocks, ship's stores, and machinery spaces

These measures aim to prevent unauthorised access to vital areas on the ship, including accommodation blocks, ship's stores, and machinery spaces. This is crucial to thwart petty theft, hijacking attempts or hostage situations. The following guidance assumes the initial defence layer has been breached, allowing intruders onto the deck.

### Exterior doors

- **Hardened doors:** doors and frames should be hardened with extra locks.
- **Improvised security:** use door wedges, wedge braces, door locking bars, scaffold supports, pallets, and wire strops to secure doors. For example:
  - Door wedges: prevent doors from opening by placing wedges at various points.
  - Wedge braces: secure doors with braces that fit over the handle and brace against the door.
  - Locking bars: install bars across door frames to protect against forceful entry.
  - Scaffold supports: use props to brace doors facing strong points.



  - Wire strops and turnbuckles: secure hatches and skylights.

So far as is appropriate, in terms of emergency access, all doors should remain closed and locked when operating in a threat area. A single point of controlled access should be designated if working on deck is necessary. As part of the handover routine, it is suggested the Officer of the Watch (OOW) checks all doors have been secured. Some doors such as the galley door, engine room door (both of which are generally located on the aft of the ship) and skylights are high-risk openings and should not be left open to vent built up heat.

### Internal doors

- **Installation:** fit secondary doors at access points in the accommodation block and engine room.
- **Design:** these doors should present a smooth surface with no handles, hinges or locks visible from the outside. They should be strong enough to withstand a physical assault and be secured from the inside. Consider locking bars on internal doors between the bridge and accommodation.
- **Citadel:** if not installed at the accommodation block, secondary doors should be fitted to the citadel, offering a final layer of defence.

### Windows

There is little point in preventing or slowing access to the accommodation block through the doors if intruders can get in by simply breaking a window or porthole.

- **Hardening windows:** fit windows and portholes with deadlights or blank covers, especially those accessible from the outside.

- **Bars:** install a minimum of three bars on large windows and ensure escape windows are easily opened in emergencies.

### Staircases, hatches, vents, and ladders

- **Hinged metal plates:** fit plates on outside staircases and ladders to obstruct climbing, without compromising crew safety.
- **Pipework protection:** install spikes or angled baffle plates on scupper pipes, fire mains, or external cable runs to prevent them from being used as climbing aids.

### Enhanced bridge protection

- **Window protection:** apply approved blast-resistant film to bridge windows.
- **Metal plates:** installation of fabricated metal plates on bridge windows and wing doors for quick deployment during an attack can be considered.
- **Chain link fencing:** use to mitigate RPG effects. Not effective if placed close to the bridge windows.
- **Sandbags/water drums/steel plate:** place on bridge wings for additional ballistic protection, checking regularly for degradation.

### 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

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.




### Internal smoke cannons, strobe lights and noise makers

- **Purpose:** these devices serve as a barrier within the accommodation block.
- **Installation:** fit smoke cannons, strobe lights and noise makers in compartments or alleyways.
- **Activation:** can be activated remotely or automatically.
- **Effect:** smoke cannons fill spaces with non-toxic smoke to disorient intruders, while strobe lights and loud horns further increase disorientation.

### Lift shafts

- **Security measure:** prevent intruders from using lift trunking to access the engine room by stopping and isolating the lift at the ship's upper deck.
- **Emergency escapes:** ensure that personnel can escape from lift trunking in emergencies but prevent intruders from entering.

### Security muster points and citadels

The company risk assessment and planning process should identify the location of security muster points within a ship and ensure crew are familiar. These will vary depending on the threat, i.e. threat from piracy (citadel), threat from WBIED/UAV (above waterline). Crew should always muster with appropriate PPE; additional PPE should be available.

### Security muster points

- **Definition:** a designated area providing maximum physical protection for the crew.
- **Location:** should be above the waterline if there's a risk of hull breach. The central stairway, protected by the accommodation block and above the waterline, is often suitable as multiple escape routes are available. Avoid spaces with windows.
- **Explosion risk:** consider potential blast paths from explosive devices when selecting the location, i.e. an armour-plated door at the bottom of the central stairwell will reduce the effect of a blast from a WBIED. All loose items at muster points should be secured to prevent additional hazards.



**ATTENTION**

**If a crew member is unable to reach the security muster location, they should find a protected location and adopt the brace position against a bulkhead.**

### Citadels

- **Purpose:** a secure location where the crew can retreat if intruders board the ship.
- **Size and facilities:** should accommodate the entire crew and any extra staff for 3-5 days. Must include communication systems (VHF and SATCOM), independent power supplies, bottled water, food and sanitation.
- **Communication:** two-way communication with company HQ and naval/law enforcement forces is essential. VHF for local and SATCOM for global communication. Satellite antennae must be independent from bridge systems.
- **Control from citadel:** ability to control propulsion and steering from the citadel could be critical under specific circumstances. If additional navigation equipment including GNSS, radar display, ECDIS and engine controls are provided in the citadel it should only be used for sailing away from imminent danger. If this is not available, the ship should be stopped prior to entering the citadel.
- **Awareness:** CCTV monitoring from the citadel will provide situational awareness and may provide footage direct to shore ship management. Consider placing the CCTV recording unit in the citadel to prevent damage by intruders.
- **Sustainability:** ensure the citadel has enough food, water, sanitary and medical supplies to sustain the crew, especially in hot climates. A clear smoking policy should be agreed and firefighting equipment available.
- **Drills and criteria:** conduct regular drills and ensure the SSP defines conditions for citadel use. Military forces may require all crew to be accounted for and in the citadel, with two-way communication, before boarding.

**ATTENTION**

**The Master should decide when to use the citadel.**



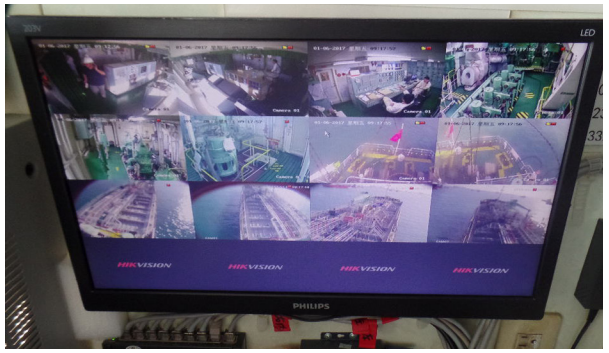

**Blackout:** electrical isolation of specific areas can disorient intruders. Electrical switchboards can create sectional blackouts without affecting the citadel/safe area.

### Fire suppression systems

- **Protection:** Secure remote activation controls to prevent intruders from misusing fixed fire suppression systems against the crew in the citadel.

### Closed Circuit Television (CCTV)

- **Installation:** provide all-round visibility with CCTV, including thermal imaging, extended memory for recording, and multiple monitor locations.
- **Discreet placement:** use discreet or disguised cameras and dummy units to mislead intruders.
- **Remote monitoring:** allow remote monitoring from the company HQ while balancing cybersecurity and privacy concerns.
- **Recording capability:** ensure the system can record and store footage for several days, aiding law enforcement in identifying intruders.
- **Audio integration:** supplement CCTV with audio devices to alert the OOW to covert intrusion attempts.
- **Install software:** to enable the transmission of CCTV images to the Company HQ if the system is disconnected.
- **Link:** the activation of the SSAS to the CCTV to allow remote monitoring from company HQ.



### Motion sensors

- **Purpose:** serve as an extra layer of hardening to warn crews of attempted or actual intrusions.
- **Types:** can be active or passive. Professional advice is recommended to determine the best type for each ship.
- **Integration:** consider location, type, coverage area, and alarm outputs when designing or retrofitting an integrated intruder detection and alert system.

### Searchlights and lighting

- **Lighting:** minimise external lighting, except for mandatory navigation lights, to prevent attackers from establishing reference points. Use searchlights to probe for suspect craft and illuminate radar contacts.
- **High-power searchlights:** utilise xenon light sources to fully illuminate and identify suspect craft quickly. High-power beams can disorient attackers temporarily.
- **Recommended lighting practices:**
  - Weather deck lighting around the accommodation block and rear-facing lighting on the poop deck to demonstrate awareness.
  - Keep searchlights ready for immediate use.
  - Switch on over-side lighting when attackers are identified or an attack commences to dazzle them and aid crew visibility.
  - Exhibit only navigation lights at night.
  - To comply with international regulations and avoid collision risks, never switch off navigation lights at night.
  - At anchor, keep deck lights on, as well-lit ships are less vulnerable to attacks.
  - Have the capability to turn off all internal accommodation lights to deter or disorient intruders.
  - Regularly maintain lighting equipment to ensure functionality.

### Securing ship's tools and equipment

- **Prevent unauthorised use:** secure all tools and equipment that could aid intruders in gaining entry. Store such items in a secure location.
- **Ballistic protection:** provide ballistic protection from small arms fire for gas cylinders or flammable liquid containers stored on the upper deck. Store excess gas cylinders securely or land them prior to transit.

### Ship-to-ship and other static operations

- These should be conducted outside increased threat areas.

### UAV mitigations

The increasing use of UAVs to cause damage to ships presents a difficult challenge for the maritime industry. An attack by UAV cannot currently be mitigated by measures deployed onboard the ship, however the effects of a UAV attack can be responded to by the crew following its emergency response procedures.

If a UAV is identified it is recommended the following actions are implemented:

- Sound alarm.
- Muster crew in appropriate PPE including hard hats in appropriate location (avoid below waterline and large amounts of glass).
- Brace for impact.
- Consider switching off AIS or other tracking communications followed by a major course alteration if safe to do so.
- Evasive manoeuvring.

In many cases multiple UAVs have been deployed against a single target ship. Repeated attacks over a period of time have also occurred.

### WBIED mitigations

WBIED can take many forms, the type of craft, control of the craft, and intent will vary. In all cases mitigations are limited however a PCASP team, if onboard, could consider use of force to try and disable the craft within their Rules of Use of Force (RUF).

### Missile mitigations

The primary mitigation for preventing missile attacks is to avoid the area completely. However, for ships transiting a missile threat area where no warning is received the ship will have to implement emergency response actions after impact. Seek military advice on the use of electronic emissions, especially AIS, if operating in areas with a missile threat.

### Sea mines

Avoid all published or identified mine danger areas and maintain close liaison with military authorities. If operating near mine danger areas, Masters should be aware of the possibility of drifting mines. Effective lookouts are essential. Where the mine is not observed prior to impact emergency response procedures should be activated.

### Helicopter boarding mitigations

It is likely this tactic would only be deployed by a state actor, therefore mitigations for the prevention of such a boarding should only be deployed where it has been validated that there is a credible threat against the ship.

If the threat has been confirmed the following may be considered to prevent a helicopter landing or fast-roping/abseiling:

- Use foam monitors to spray the deck and to create water mist.
- Fouling of the helipad and open decks with nets, place obstructions on open decks to prevent landing.
- Commence evasive manoeuvres to move abseil ropes away from the ship.
- Steam towards territorial waters at full speed.
- Course alteration to maximise rolling of the ship.

To prevent the risk of escalation, on board private security teams should not attempt to engage state actors with weapons.

### Passage coordination and military protection

Passage coordination schemes are established by military forces to facilitate coordination between the operational commanders of military assets and one or more merchant ships intending to transit a specific area or route. The primary objectives of these schemes are deterrence and protection, including mutual protection among merchant ships.

### Key points:

- Legal constraints:
  - Escorting military assets may be legally constrained under international law, Military Rules of Engagement (ROE), and national caveats.
  - Military assets may not be able to actively protect merchant ships under attack unless responding under the inherent right of self-defence as permitted by international law.
  - ROE are determined at the political/strategic military level and communicated to the Military Commander.

- Resource limitations:
  - There may be insufficient military assets available to escort all merchant ships within the military area of operations.
  - Prioritisation of ship passage may be necessary due to limited resources.

- Master's responsibility:
  - Passage coordination does not relieve the Master of their responsibility for the safe navigation of the ship.
  - Merchant ships remain under the command of their Masters and not under military control, though they may receive routing and navigational guidance as well as threat information during a group transit period.

These schemes aim to enhance the safety of merchant ships through coordinated efforts without compromising the autonomy and responsibility of the ship's Master.

### Engaging Private Maritime Security Companies (PMSC)

BMP does not recommend or endorse the general use of armed security personnel or Security Escort Vessels (SEV) to safeguard merchant ships; this is a decision taken by individual ship operators. Employment of PMSC services should be an output of the threat and risk assessment and consider the factors outlined below.

Shipping companies should only employ PMSCs certified to the current ISO 28007-1:2015 *Guidelines for Private Maritime Security Companies*. A PMSC contract should:

- Be between the technical manager and the PMSC.
- Not prejudice the ship's insurance cover arrangements.

- Ensure the PMSC has current and compliant insurance policies.
- Clearly identify the procedure for the use of force.
- Confirm the Master's overriding authority.
- Include a medical clause in case a team member provides first aid to a crew member.

### Privately Contracted Armed Security Personnel (PCASP)

PMSCs may offer both armed and unarmed services. While it is acknowledged that the presence of PCASP has been effective, their presence could increase HSSE risks due to there being weapons onboard. This should be considered in the risk assessment. The decision to engage a PMSC is left to individual ship operators, subject to the permissions of the ship's Flag State and any littoral states.

### Considerations for engaging a PMSC

- **Current threat and risk environment:** evaluate the prevailing security threats and risks in the area of operation.
- **Company risk assessment:** use the output of the company's risk assessment to inform the decision.
- **Voyage plan requirements:** assess the specific needs of the voyage, including route, duration, PCASP transfer and their logistics onboard.
- **Ship characteristics:** consider ship speed, freeboard, and type of operations (e.g., seismic survey, cable laying).
- **Existing protection levels:** review the levels of protection provided by navies, coastguards and maritime police in the operating area.

### Documentation requirements for PCASP

If the decision is made to deploy a PCASP, the following documents will be required:

- **Letter of authorisation:** obtain a letter from the Flag State confirming that the use of armed guards is permitted.
- **P&I Club letter:** secure a letter from the Protection and Indemnity (P&I) Club stating that the employment of PCASP does not prejudice the P&I cover.
- **War risk assurance letter:** acquire a letter from war risk insurance broker confirming that armed guards are permitted with no change in cover.

### Master's overriding authority

If private security contractors are embarked, there must be a clear understanding of the Master's overriding authority. The Rules for the Use of Force (RUF) under which the PCASP operates 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 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 the crew and ship.

PCASP should be used only as an additional layer of mitigation and protection, not as an alternative to other measures. The decision to carry PCASP is an output of the risk assessment.



**ATTENTION**

**The ship's crew must not handle or use firearms.**

These considerations and documentation requirements ensure that the engagement of PMSCs is conducted within legal frameworks and does not compromise the ship's insurance coverage.

Refer to the PMSC guidance paper at www.maritimeglobalsecurity.org.

## Security Escort Vessels

### West Africa – Security Escort Vessel (SEV) considerations

SEVs are privately contracted vessels used to escort/protect ships usually within the EEZ and territorial waters of a coastal state. The intent is for the presence of embarked military and security personnel onboard an SEV to discourage piracy and criminal attacks.

When selecting an SEV, compliance and assurance checks with the PMSC/SEV provider should include:

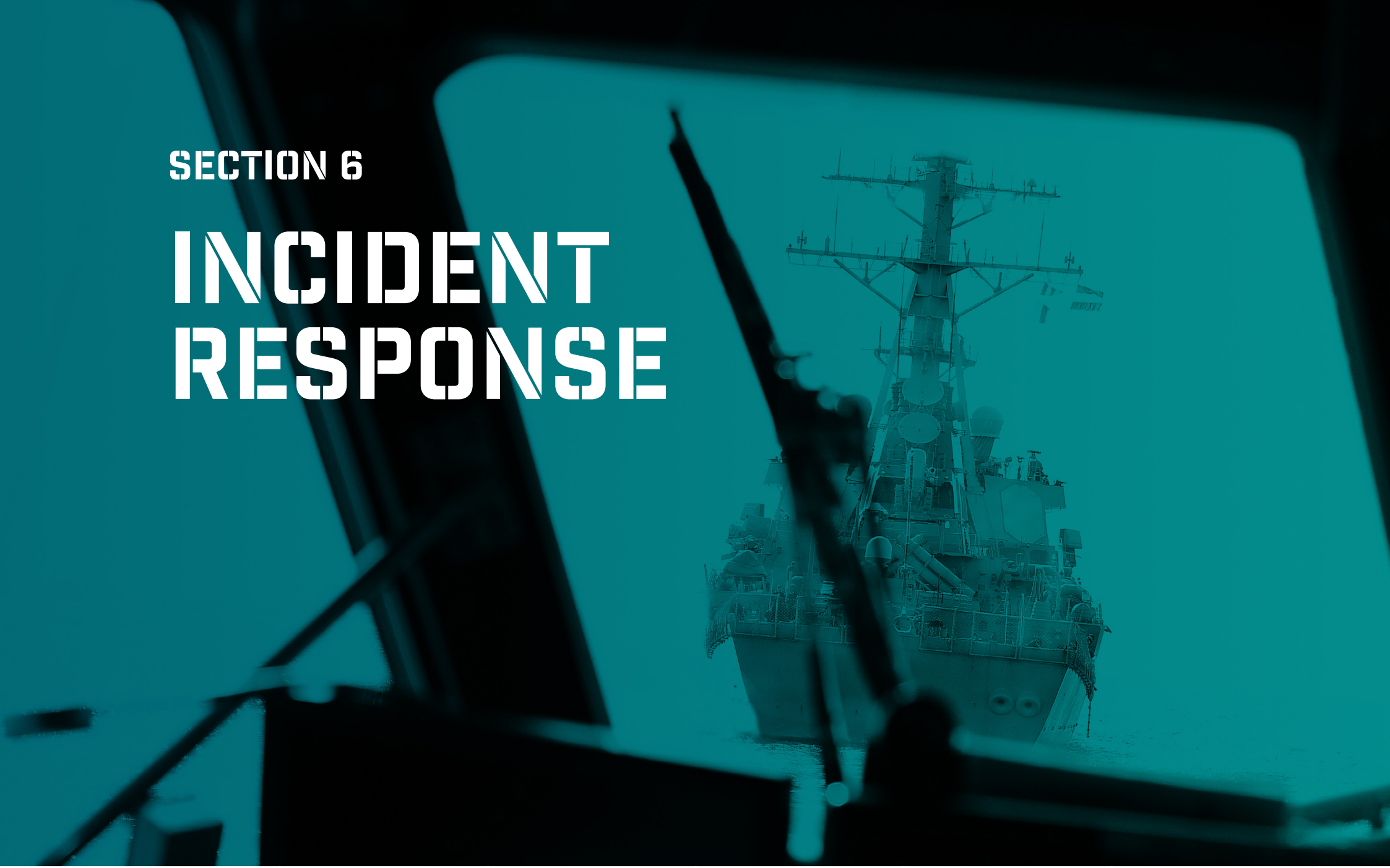
1. **SEV classification details:** obtain recent dated photographs of the SEV.
2. **Certificate of Ownership and Registry:** request the SEV's official documents.
3. **Maintenance report:** request the SEV's latest maintenance report or, if sub-chartered, the PMSC's due diligence audit report.
4. **Evidence of recent sea trial:** obtain an AIS screenshot of a recent escort showing the SEV's speed, date and coordinates.
5. **MoU and Service Agreement:** where required request a copy of the Memorandum of Understanding between the Navy and the SEV operator under which the SEV operates, along with the PMSC's Joint Venture Service Agreement with the SEV owner/provider.
6. **National Navy approval:** request a copy of the appropriate Navy approval letter or email for Navy personnel to operate on the SEV.
7. **Insurance documents:** obtain a copy of both the SEV's hull insurance and the PMSC's liability insurance.
8. **Master's feedback:** request recent feedback on the SEV's last escort performance.
9. **OVID certificate or CMID:** obtain an Offshore Vessel Inspection Database certificate or Common Marine Inspection Document.
10. **Routing:** the PMSC should provide a threat assessment for the route and SEV rendezvous point.

It should be noted that the use of onboard private armed security teams may be prohibited within some jurisdictions.



SECTION 6

# INCIDENT RESPONSE



# Incident response

There are a variety of security incidents a ship could encounter when transiting a threat area, and a proportionate and dynamic response is critical in mitigating their potential impacts. The following sections explain the measures that should be applied by shipboard personnel in the event of specific maritime security incidents. The threats described have all been encountered by ships in recent years.

## General guidance

Ships should have well practiced plans for emergency response to security incidents. Ships should refer to the bridge cards for initial actions.

When operating in an area of conflict, emergency response should be conducted using normal response processes with military or private security incorporated into the response to provide appropriate support.

## Illegal boarding

Attackers will approach the ship with an intent to board from the sea. The intent of such attacks varies; pirates will typically seek to kidnap seafarers, while others such as military or paramilitary personnel may seek to hijack ship and crew for political gain. Despite these differing motivations, the characteristics of such attacks are similar, as are the recommended mitigation measures.

Attackers from sea typically open fire as they approach the ship to induce fear and get the ship to slow down or stop. Use any available time to activate additional protective measures and plans. This signals to the attackers that the ship is prepared.

### Approach stage

Effective and properly equipped lookouts are the best aid in identifying the nature of an attack. The threat profile of attacks may initially look similar, and it may not be until the attacking ship is close that the nature of the attack becomes apparent. In all cases, the following steps should be taken:

1. **Increase speed:** if not already at full speed, increase to maximum to open the distance.
2. **Steer straight:** maintain a straight course to sustain maximum speed.
3. **Initiate emergency procedures:** activate the ship's emergency procedures.
4. **AIS considerations:** implement the Automatic Identification System policy.
5. **Emergency communication:** activate the emergency communication plan, sound the emergency alarm, and make an attack announcement per the ship's emergency communication plan.
6. **Mayday call:** make a mayday call on VHF Channel 16. Send a distress message via the Digital Selective Calling (DSC) system and recognised mobile satellite service, as applicable.
7. **Activate SSAS:** ensure the Ship Security Alert System is activated.
8. **Report the attack:** immediately report the attack to relevant authorities.
9. **Security Escort Vessel:** if accompanied by an SEV, consider its speed capabilities and ability to keep up. A decision to stay or leave, with the SEV should be considered.



10. **Water spray:** activate water spray systems.
11. **Secure doors:** ensure all external doors and, where possible, internal public rooms and cabins are fully secured.
12. **Crew muster:** all crew not required on the bridge or in the engine room should muster at the security muster point or citadel as instructed by the Master.
13. **Course alteration:** when sea conditions allow, consider altering course to increase an approaching skiff's exposure to wind/waves.
14. **Sound whistle/foghorn:** sound the ship's whistle or foghorn continuously to demonstrate to potential attackers that the ship is aware of the attack and is reacting to it.
15. **VDR recording:** save the Vessel Data Recorder (VDR) recording.
16. **PCASP actions:** PCASP, if present, will take agreed actions to warn off attackers according to the RUF.

### Attack stage

As attackers get closer, the following steps should be taken:

1. **Reconfirm crew location:** ensure all crew members are at the security muster point or citadel as instructed by the Master. In the case of piracy, the crew should NOT leave the citadel until they have confirmed pirates have left the ship or the military provide a 'safe word' – this could take days.
2. **Helm alterations:** commence small helm alterations while maintaining speed to deter skiffs from lying alongside the ship in preparation for a boarding attempt. Large amounts of helm alterations are not recommended as they may significantly reduce the ship's speed.

### Actions on illegal boarding

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

- **Stop the ship:** take all way off the ship and stop the engines.
- **Muster crew:** all remaining crew members should proceed to the citadel or security muster point; the last crew member should lock all internal doors on route.
- **PCASP procedures:** PCASP, if present, will follow procedures agreed with the company and Master.
- **Ensure crew presence:** prior to securing doors, ensure all crew are present in the citadel or security muster point, including the Master, bridge team, and PCASP. Implement agreed actions if a crew member is unable to reach the citadel.

### Actions on illegal boarding by state representatives/paramilitary forces

Ships operating in the Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea and Red Sea have been boarded by state security forces. If hailed by security forces, ships should provide their name and Flag State and affirm they are proceeding under international law and consider the following:

1. **Maintain distance:** ships should stay as far as possible from territorial waters without compromising navigational safety.
2. **Decline boarding:** if security forces seek to board, the Master should decline permission if it does not compromise the safety of the ship and crew, noting adherence to international law.
3. **Non-resistance:** if security forces illegally board the ship, the crew should not forcibly resist.
4. **Immediate reporting:** in the event of suspicious activity or doubt, call the relevant authorities immediately.



### DO:

Prepare the ship's crew to cooperate fully during any state or military action onboard:

- Keep low to the deck and cover your head with both hands.
- Keep hands visible.
- Be prepared to be challenged on your identity.
- Be prepared to be separated based on identity/nationality.
- Cooperate fully with state or military forces.



### DON'T:

- Make movements that could be interpreted as aggressive.
- Take photographs.
- Engage in ship activities unless instructed by military personnel.

### Control of ship lost/hijack – hostage situation

In the event of a ship hijacking and holding the crew the following principles serve as guidelines:



## DO:

- **Remain calm:** maintain self-control.
- **Be respectful:** be humble, respectful to captors and do not get involved or affected by prejudice-based treatment.
- **Look out for colleagues:** ensure the well-being of colleagues.
- **Stay together:** stay together as a team where possible.
- **Accept leadership:** accept the new leadership and maintain the hierarchy of rank.
- **Communication:** try to establish normal communication with the captors.
- **Hygiene:** maintain personal hygiene.
- **Conserve resources:** save water and essentials.
- **Stay positive:** many people are working to release you.
- **Be patient:** maintain routines, including spiritual needs.
- **Regular breathing:** keep your breathing regular to help stay calm.
- **Mental activity:** meditate or keep mentally active.
- **Respect religion:** respect your religion, colleagues', and captors'.



## DON'T:

- Offer resistance.
- Argue with captors or colleagues.
- Take photographs.
- Hide valuables.
- React emotionally.
- Take drugs or alcohol.
- Bargain for personal privileges.

### Actions on boarding by activists

Activists have a history of conducting well planned and executed boardings on vessels and offshore platforms. Such boardings are generally peaceful and aimed at gaining media attention – often by attaching banners and filming the event. These actions are commonly supported by a mothership, which may also record the activity and deploy UAVs (drones).

It is essential that crews are properly briefed, trained, and regularly practise their response procedures as such boarding incidents have potential to produce numerous safety incidents.

On platforms, protestors typically move to a high point in the structure to make removal more difficult.



## DO:

- Consider activism in the threat assessment.
- Report immediately to the CSO/Shore authority/Flag State.
- Activate vessel operator's plan to support vessel personnel in responding to protesters.
- Stay calm and professional.
- Secure access points as soon as an approach is identified.
- Consider using a loudhailer and prepared statements to address approaching protestors.
- Ensure the safety of the vessel, crew, and embarked protestors.
- Respond quickly and establish communication to understand protestor intentions.
- Communicate safety rules and highlight unlawful actions.
- Plan for additional personnel resources to manage the protest.
- Consider nominating a Protest Response Team and using a roster to manage fatigue.
- Brief crew and instruct them not to film or post on social media.
- Observe and document the boarding.
- Assign a crew member to record/photograph if safe to do so.
- Add number of protesters to the POB/Passenger list.

- Request to check bags for items that may affect ship safety.
- Request protesters wear PPE.
- Assign a safe area for their stay.
- Consider if electronic devices bought on board pose a potential ignition risk for the vessel/platform.
- Clearly communicate to the protesters any safety or environmental pollution concerns related to the protesters' actions.

## DON'T:

- Deploy technical anti boarding measures such as razor wire or water cannons.
- Interfere with or disable UAVs.
- Conduct evasive manoeuvres if the boarding vessel is close.
- Engage in physical confrontation with boarding or onboard protesters.
- Share personal information with the protesters.

### Equipment considerations

- Megaphones/loudhailers.
- Safety PPE and blankets for up to ten protesters.
- High visibility jacket labelled Master/OIM.
- Video camera, smartphone, audio recording equipment (certified for use in hazardous areas)
- Laminated prepared statements regarding safety/emergencies, etc.
- Laminated vessel safety induction information.
- Headtorches to support safe movement in an emergency.
- Water bottles.
- Heavy duty scissors to remove banners/placards (consult shore authority before acting).

### Following departure

- Conduct a thorough sweep of the vessel/platform.
- Search for unauthorised personnel and/or suspicious items/packages and signs of damage.

## Missiles

Where a warning is received, and time permits, the following should be considered:

- Sound appropriate alarm.
- Muster crew in appropriate PPE including hard hats in appropriate location (avoid below waterline and near large amounts of glass).
- Consider switching off AIS or other tracking communications.
- Change course to minimise the profile of the ship to the direction of the threat.
- Activate emergency response procedures.
- Brace for impact.

## Sea mines

If a look out observes a sea mine, consider the following:

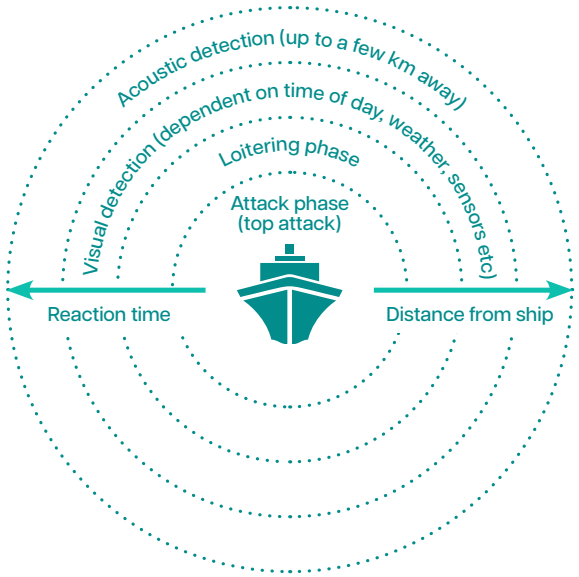
- Alter course to avoid mine.
- Sound appropriate alarm.
- Close watertight doors and consider blast route.
- Muster crew in appropriate PPE including hard hats in appropriate location (avoid below waterline and large amounts of glass).
- Post extra lookout to look for additional mines in the vicinity.
- Note position and issue VHF warning.
- Activate Emergency Response procedures.
- Brace for impact.



### UAV attack

It is very difficult to detect a UAV. If a UAV is heard or identified, consider the following:

- Sound appropriate alarm.
- Consider switching off tracking communications, e.g. AIS.
- Muster crew at the appropriate security muster point.
- Time permitting, close all fire screen doors.
- Brace for impact.




### WBIED attack

In the early stages of an attack, it may not be possible to distinguish between an illegal boarding or WBIED. Initial actions for illegal boarding should be followed. WBIEDs are usually unmanned, but some variants use crew until the final approach and others use dummies to mask their intent. It is recommended that if the WBIED is identified the following is implemented:

- Sound appropriate alarm.
- Consider turning towards the threat to avoid a strike to the engine or steering gear compartments.
- Muster crew at the appropriate security muster point (avoid below waterline and near large amounts of glass).
- Brace for impact.

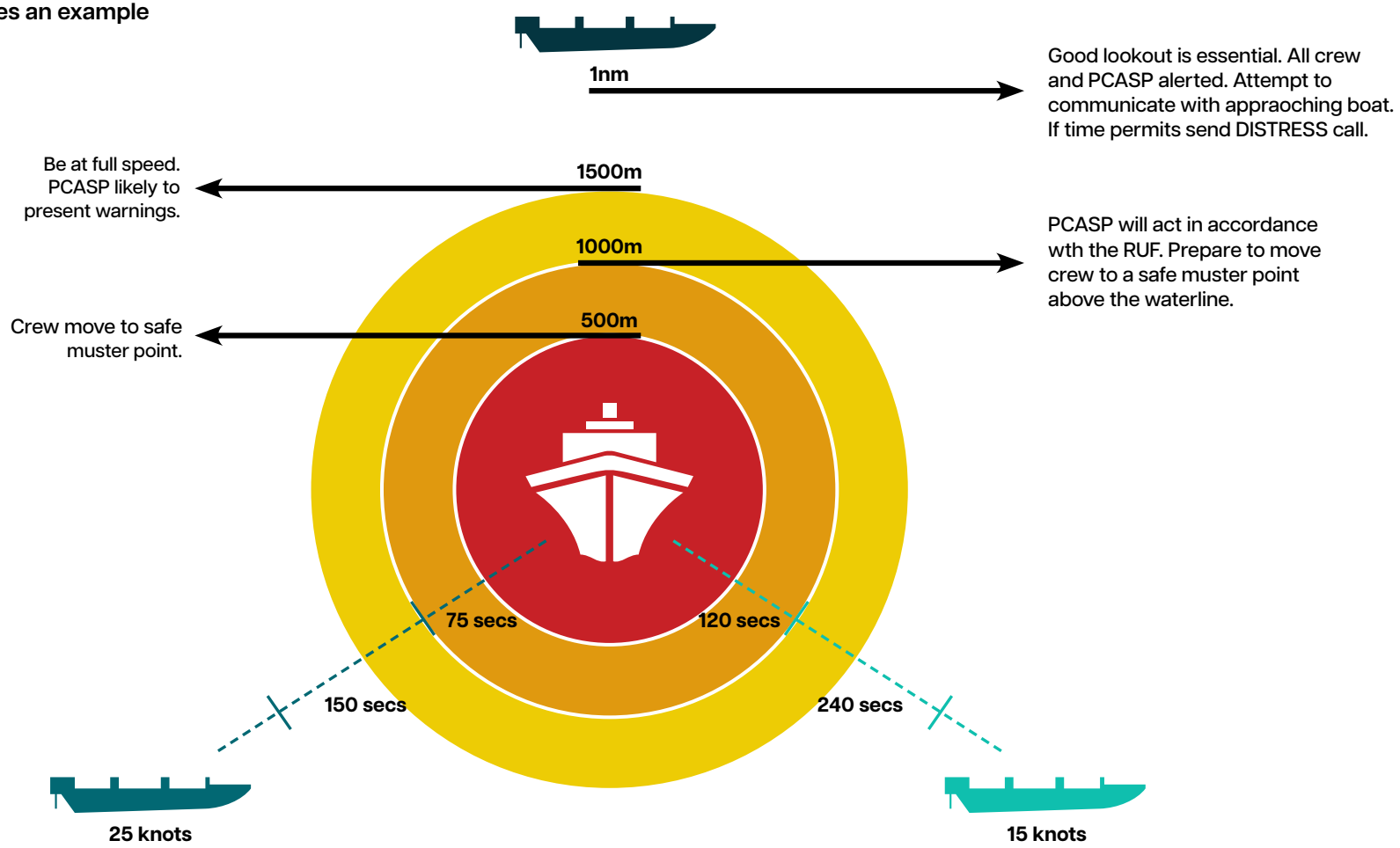
### The brace position

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.

Keeping the mouth open may reduce shock wave damage to the ears.



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



SECTION 7

# POST-INCIDENT PROCEDURES



# Post-incident procedures

A comprehensive plan to account for personnel, assess damage and collect evidence is crucial. The wellbeing of seafarers must be prioritised. Once all attacks are confirmed as complete, it is important to follow these guidelines:

## Actions post-attack

- **Send distress signal:** immediately send a distress signal if not already sent.
- **Account for personnel:** ensure all crew and PCASP are accounted for.
- **Administer first aid:** provide medical support to any injured crew members.
- **Notify stakeholders:** call the CSO and relevant authorities.
- **Implement damage control:** take necessary actions to control and mitigate damage following ship's emergency procedures.
- **Survey damage area:** inspect the area where the blast or attack occurred.
- **Save VDR:** save and transmit (if possible) VDR data to managing office.
- **Preserve evidence**: restrict access to area and control scene in preparation for evidence collection by authority.
- **Media:** prepared guidelines on how to interact with media post-incident may help prevent misinformation.

## Post-attack recovery

The period following an attack will be challenging as the company, Master and crew recover from the ordeal. It is essential that seafarers receive timely and proper medical assessments, both physical and mental, and care. Companies should have emergency management plans in place to manage the effects of an attack, including handling long, drawn-out hostage negotiation situations and supporting the families of those affected by a threat incident, including piracy or armed robbery.

## Unexploded ordnance and projectile materials

If a ship is attacked by a UAV, missile or similar projectile it is possible the munition may not explode leaving Unexploded Ordnance (UXO). If a projectile impacts a ship but does not explode the crew should:

- Secure the impact area and maintain a safe distance.
- Avoid the use of UHF/VHF and other transmitting devices in the vicinity.
- Preserve the area of impact and all evidence without touching or dismantling debris.
- Avoid contaminating the evidence and do not clean the area.
- Take initial statements or observations from the crew.
- Take photographs of the crime scene from multiple viewpoints.
- Protect the VDR for future evidence.
- Seek military advice for the disposal of debris.



**WARNING**

**Any radio emissions in proximity may trigger UXO.**

### Evidence preservation and collection

To give investigating authorities the best chance of apprehending the perpetrators, it is important that evidence is preserved correctly. Companies, Masters and crew should refer to the IMO Guidelines on Preservation and Collection of Evidence (A28/Res.1091).

1. **Detailed reporting:** following any attack or suspicious activity, a detailed report should be completed and sent to the company, the Flag State and appropriate authorities. This report should be comprehensive and include supporting evidence and witness statements.

2. **Protecting the crime scene:**
   - Preserve the crime scene and all evidence.
   - Avoid contaminating or interfering with evidence; if in doubt, do not touch and leave items in place.
   - Do not clean the area or 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 the 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 interviews by law enforcement authorities.

### Investigation process

Thorough investigation using all available evidence is critical. The quality of the evidence provided and the availability of the crew to testify significantly aid any investigation or prosecution. The investigating authority will depend on various factors such as the Flag State, ownership, and crew nationality. Statements from the ship's Master and the PCASP provide crucial evidence.

### Additional support and advice

INTERPOL provides support to ship operators who have experienced hijacking. Its Maritime Security Unit can provide advice on preserving the integrity of evidence left at the crime scene and liaising with the appropriate agencies. Contact can be made via INTERPOL's 24/7 Command and Coordination Centre (CCC) at os-ccc@interpol.int.

### Seafarer treatment

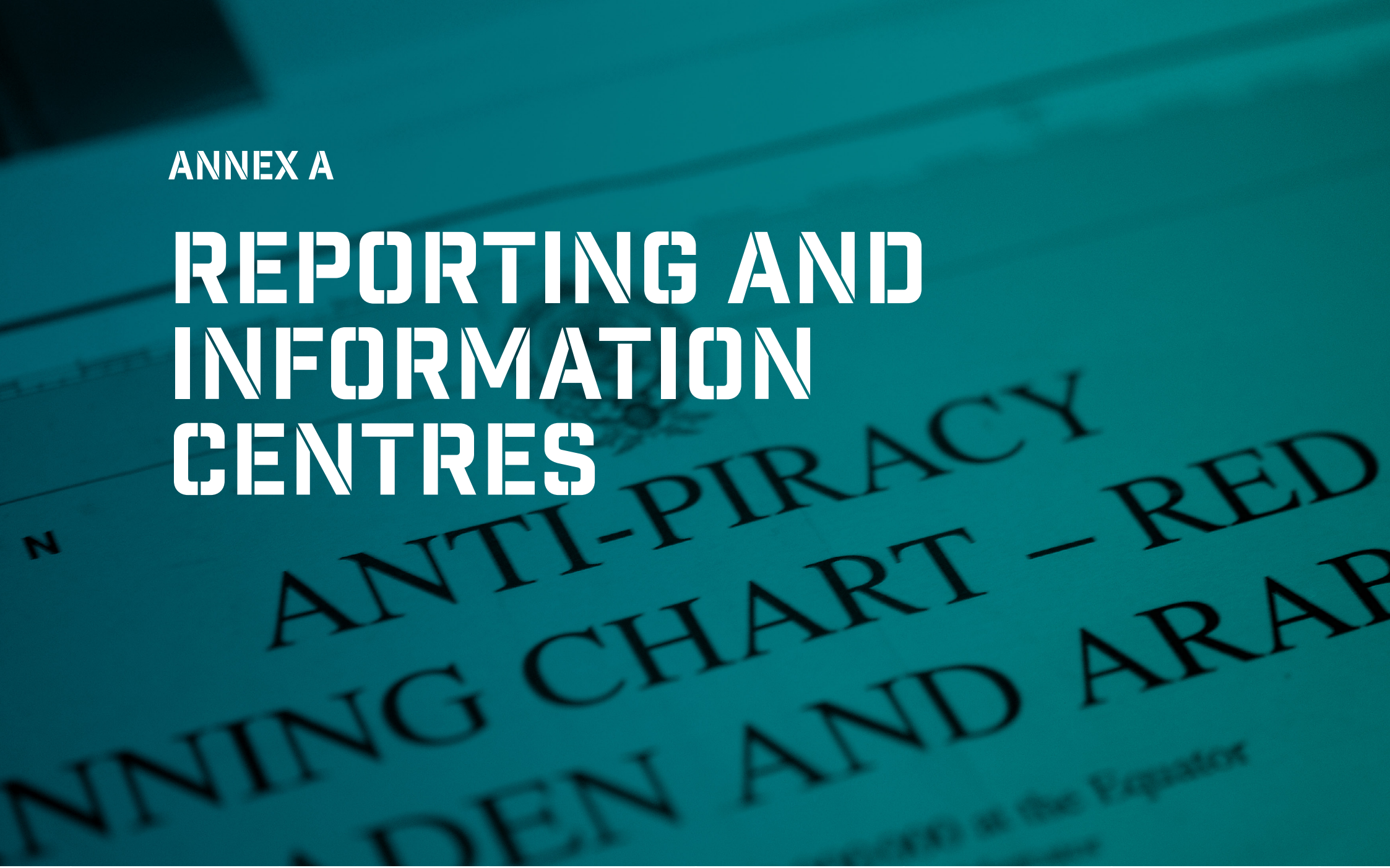
Seafarers should always be treated with respect and as victims of crime. Law enforcement agencies will talk to the Master and crew to understand the event sequence and circumstances. In post-hostage situations, authorities may conduct post-release crew debriefs and collect evidence for investigations and prosecutions.

### Seafarer welfare

Seafarers and their families often struggle to express or recognise the need for assistance after exposure to security threats. Details on supporting organisations for seafarers is at annex B.

ANNEX A

# REPORTING AND INFORMATION CENTRES



# Annex A – Reporting and information centres

## Overview

Masters are strongly encouraged to inform regional and military organisations of their movements to aid situational awareness and incident response. Continuous reporting is essential once a ship has commenced its passage. Companies should identify regional reporting requirements during the risk assessment process and include requirements in voyage orders.

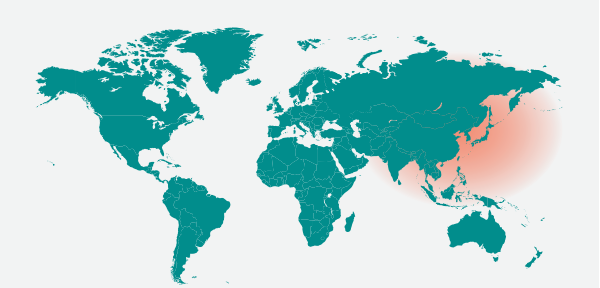
Annex B includes the contact numbers and email addresses for networks that support seafarer welfare and wellbeing.

## Maritime Reporting Centres

Various centres worldwide facilitate maritime reporting, helping enhance security and response to incidents effectively. They do not replace the role of any Maritime Rescue Coordination Centre (MRCC) whose details are available in the IMO's Global Search and Rescue (SAR) Plan. Key maritime security reporting centres and their contact details follow:

### International Maritime Bureau (IMB)

- **Role:** the IMB is a non-governmental and not-for-profit organisation which acts as a 24/7 single point of contact for reporting incidents of piracy or robbery around the globe.
- **Services:** the IMB relays information to and requests help from law enforcement and navies to assist ships. The primary working language of the IMB is English, the team however has a multilingual capability. Warnings and advice related to piracy and robbery incidents are also broadcast via Inmarsat and Iridium to ships and via email to CSOs. The IMB regularly participates in security/emergency drills with ships and provides routing advice related to waters prone to incidents of piracy and armed robbery.
- **Contact:**
  Email: piracy@icc-ccs.org
  Tel: +603 2031 0014
  Whatsapp/Telegram: +60 11 2659 3057
  Website: icc-ccs.org/piracy-reporting-centre




### Information Fusion Centre (IFC) – Singapore

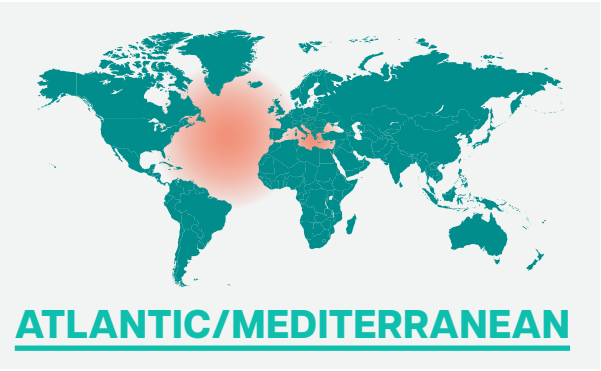
- **Role:** Regional Maritime Security (MARSEC) information-sharing hub.
- **Services:** Facilitates information sharing, provides MARSEC situational awareness, cue operational responses.
- **Contact:**
  Email: ifc_do@defence.gov.sg
  Tel: +65 9626 8965 (hotline),
  +65 6594 5728 (office)
  Website: ifc.org.sg

### ReCAAP Information Sharing Centre (ISC)

- **Role:** A government-to-government international organisation established to combat piracy and armed robbery against ships in Asia by enhancing regional cooperation through information sharing, capacity building and cooperative arrangements.

- **Services:** Provides timely, accurate information and analysis of incidents to support risk assessment via the ReCAAP ISC interactive dashboard. A mobile application [ReCAAP] to report incidents directly to coastal states and focal points, and access reports, guidebooks and posters.

- **Contact:**
  Tel: +65 6376 3063
  Fax: +65 6376 3066
  Website: recaap.org




### NATO Shipping Centre (NSC)

- **Role:** NATO's primary point of contact and hub for the maritime commercial community for interaction between the shipping industry and naval forces. Host for the NATO Maritime Centre for the Security of Critical Undersea Infrastructure (NMCSCUI).

- **Services:** The NSC deploys the instruments of Naval Cooperation and Guidance for Shipping (NCAGS) and Allied Worldwide Navigational Information System (AWNIS) to de-conflict military operations and commercial activities at sea.

- **Contact:**
  Address: NATO Shipping Centre, Atlantic Building, Northwood Headquarters, Sandy Lane, Northwood, Middlesex, HA6 3HP, UK
  Tel: +44 (0) 1923-956574
  Email: info@shipping.nato.int
  Fax: +44 (0) 1923-956575
  Website: shipping.nato.int/nsc

### The Maritime Information Cooperation & Awareness Center (MICA Center)

- **Role:** The MICA Center is the French centre for analysis and assessment of global maritime security.

- **Services:** Connected to the French national operating headquarters and worldwide diplomatic network, the 24/7 MICA Center monitors, assesses and provides the maritime industry with alerts on worldwide incidents.

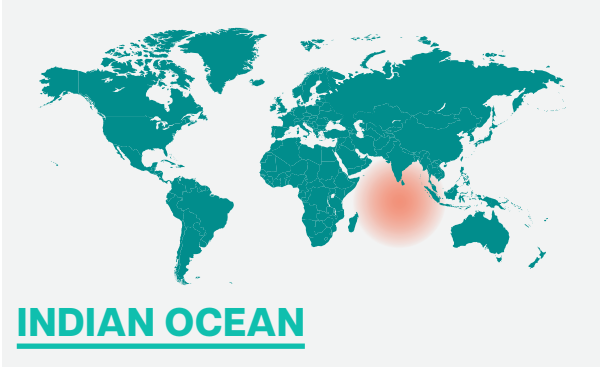
- **Contact:**
  Tel: +33 (0)298 149 917
  Email: mica-watchkeeper.fct@def.gouv.fr
  Website: fms.marine.defense.gouv.fr
  mica-center.org/




### Maritime Trade Operations Team 1

- **Role:** Protecting Australia's seaborne trade through support to military commanders and the maritime industry.

- **Contact:**
  Address: Maritime Operations c/o HMAS Moreton
  Apollo Road Bulimba QLD 4171,
  Attention: MTO Duty Officer
  Telephone: +61 (0) 431 764 980
  Email: mto.opso@defence.gov.au




### The Djibouti Code of Conduct (DCOC)

DCOC is a network to exchange information on piracy incidents across the region and other relevant information to help shipping and signatory states.

- **Role:** Maritime centres monitor the maritime domain for situational awareness and potential threats.

- **Services:** 24/7 service to respond and provide timely reports on incidents at sea to all seafarers and signatory states.

### Information Fusion Centre – Indian Ocean Region

- **Role:** To strengthen maritime security in the Indian Ocean region by maintaining a maritime situational picture and promoting information sharing.

- **Services:** To disseminate maritime security information, analysis, and advisories through its website and coordinate with other centres as well as maritime forces to support operations to counter piracy, smuggling, hybrid attacks and maritime incidents.

- **Contact:**
  Address: Sohna Road, Sector 33, Gurugram 122002, India
  Email: ifc-ior.gurugram@nic.in
  Tel: +91-124-2208385, +91-8527599898(c)
  Fax: +91-124-2209385
  Website: ifcior.indiannavy.gov.in
  X: x.com/IFC_IOR

### Regional Centre for Operational Coordination (RCOC)

- **Location:** Seychelles

- **Contact:**
  Address: P.O Box 1427, Regional Maritime Security Bodies, Ex-Coast Guard Base, Bois de Rose, Victoria, Mahe, Republic of Seychelles
  Tel: +248 4385669
  Email: rcocwatchflor@gmail.com
  Website: x.com/RCOC_Center

### Regional Maritime Information Fusion Centre (RMIFC)

- **Location:** Madagascar

- **Contact:**
  Address: Bâtiment CFIM au rez-de-chaussée, Ankaditoho, Soanierana , Antananarivo, Madagascar
  Tel: (+261) 020 22 24 393 / (+261) 33 14 028 89 / (+261) 34 90 338 12
  Email: directeur.general@crfimmadagascar.org
  X: x.com/rmifcenter?s=11&t=5zxfXC6pSWf8MDSEoNic2g



## LATIN AMERICA

### International Fusion Center (IFC) Peru

- **Role:** The IFC-Peru Maritime Information Fusion Center for Latin America collects and analyses timely, accurate and useful maritime information for Latin American countries, countries with scope in the IFC-Peru's area of interest and the international maritime community, with the purpose of issuing periodic reports, focused on increasing safety and security in the aquatic environment; and integrating capabilities to face common threats, through interoperability and information exchange with other similar centres worldwide.

- **Services:** Enhances safety and protection, integrates capabilities to face common threats in the aquatic environment.

- **Contact:**
  Email: ifc.peru.latinoamerica@gmail.com
  Tel: +51913862174
  Website: dicapi.mil.pe/ifc-latam-peru



## MIDDLE EAST

### EU Maritime Security Center – Indian Ocean (EU MSC-IO)

- **Role:** The EU Maritime Security Centre Indian Ocean (EU MSCIO) supports Operations EUNAVFOR ATALANTA and ASPIDES by collecting, analysing, and providing actionable maritime security information across the Red Sea, Gulf of Aden, Western Indian Ocean, and Persian Gulf.

- **Services:** EU MSCIO provides 24/7 assistance through its website, issuing alerts, regular threat assessments, and incident-specific bulletins to help secure merchant vessels. The centre promotes information sharing and offers protective measures, contributing to the freedom of navigation.

- **Contact:**
  Tel: +33 (0)298 220 220 (24/7) / +33 (0)298 220 170
  Email: postmaster@mscio.eu
  Website: mscio.eu

### Joint Maritime Information Center (JMIC)

- **Role:** Identify, fuse and distribute information to the global maritime community of interest with a focus on disruption to the freedom of navigation in the Middle East region.
- **Services:** Provide timely and factual event driven products and assessments, offering advice, and where prudent, military guidance only to help inform any threat and risk assessment process.
- **Contact:**
  Tel: TBD
  Email: JMIC.Bahrain@us.navy.mil
  Website: products may be viewed at ukmto.org/partner-products/jmic-products

### UKMTO

- **Role:** Supports maritime safety and security through incident reporting and information exchange, working closely with the MSC(IO) and JMIC and acting as a key liaison between merchant ships and military forces in the Middle East region.
- **Services:** 24/7 assistance through the Voluntary Reporting Scheme, issues verified and corroborated warning and advisories. Administers Voluntary Reporting Scheme.
- **Contact:**
  Tel: Emergencies +44 (0) 2392 222060
  Tel: Info +44 (0) 2392 222065
  Email: watchkeepers@ukmto.org
  Website: ukmto.org



## WEST AFRICA

### Maritime Domain Awareness for Trade – Gulf Of Guinea (MDAT-GOG)

- **Role:** Maintains 24/7 maritime situational awareness in the central and western African maritime areas, supports the Yaoundé Code of Conduct.
- **Services:** The 24/7 centre administers the GOG VRA. The centre informs and supports the maritime industry by coordinating with regional authorities.
- **Contact:**
  Tel: +33 298228888
  Email: watchkeepers@mdat-gog.org
  Website : gog-mdat.org/home

### Yaoundé Architecture for Maritime Security (YAMS)

YAMS is a maritime security framework, agreed by West and Central African states.

- **Role:** Each zone monitors the maritime domain for situational awareness and potential threats.
- **Services:** To respond and provide timely reports on incidents at sea to all seafarers.

### Maritime Multinational Coordination Centre (MMCC) Zone G

- **Location:** Cape Verde
- **Contact:**
  Tel: +2382633622/+2382633623
  Email: mmcczoneg.ops@gmail.com
  Website: icc-gog.org/?page_id=1575

### MMCC Zone F

- **Location:** Accra, Ghana
- **Contact:**
  Tel: +23354796523
  Email: zonefmmcc@gmail.com
  Website: icc-gog.org/?page_id=1575

### MMCC Zone E

- **Location:** Cotonou, Benin

- **Contact:**
  Tel: +229 61 04 04 75 / +229 51 99 14 25
  Email: zonee.mmcc@gmail.com
  Website: icc-gog.org/?page_id=1575

### MMCC Zone D

- **Location:** Douala, Cameroon

- **Contact:**
  Tel: +237233424001/+237233425948
  Email: cmczoned.eccas@yahoo.fr
  Website: icc-gog.org/?page_id=1575

### MMCC Zone A

- **Location:** Luanda, Angola

- **Contact:**
  Tel: +244 923 462 501
  Email: Surumba2012@gmail.com
  Website: icc-gog.org/?page_id=1575

## Additional resources

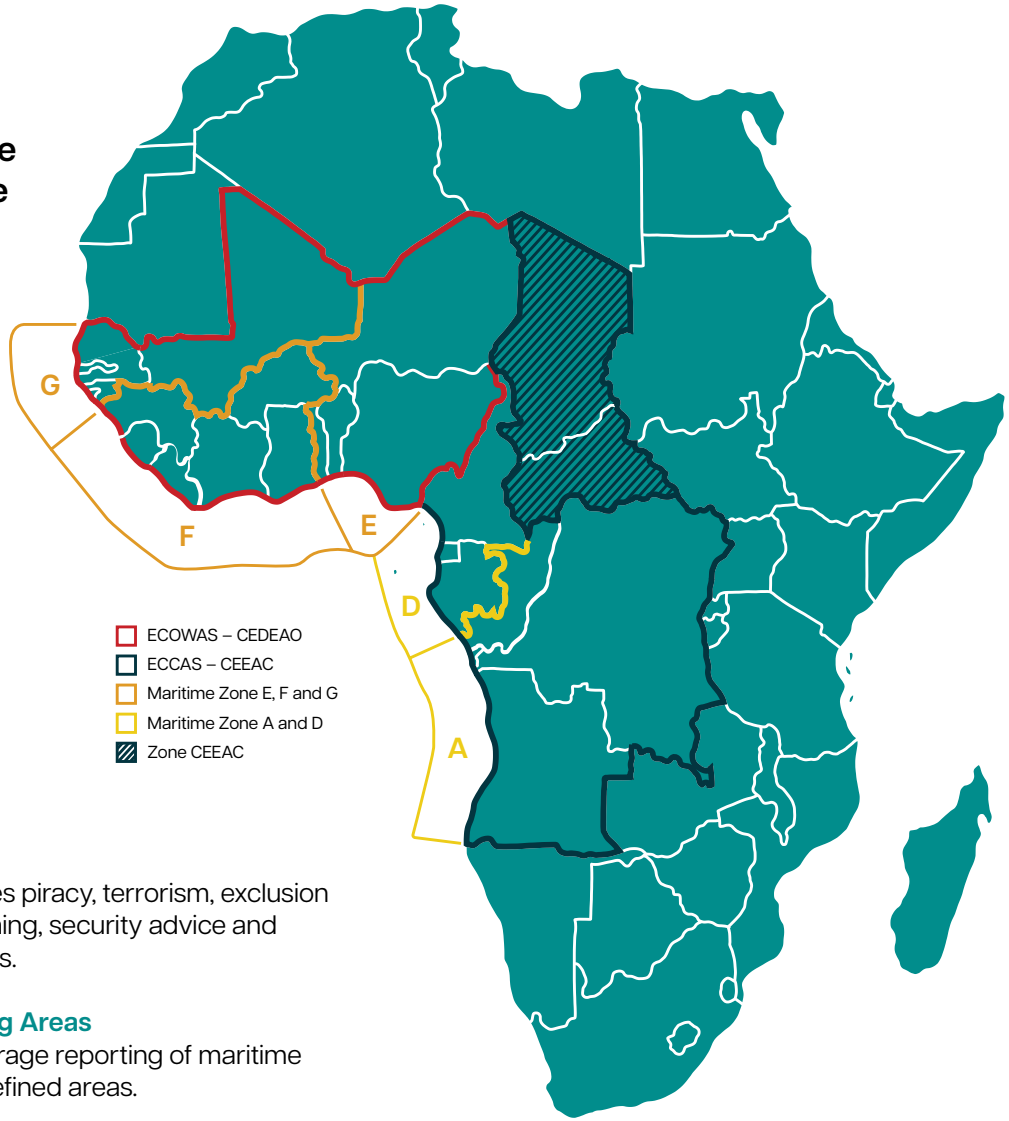
### Maritime security charts

- **Purpose:** Assist in planning voyages through high-threat areas by providing safety-critical information.
- **Content:** Includes piracy, terrorism, exclusion zones, illegal fishing, security advice and regional contacts.

### Voluntary Reporting Areas

- **Purpose:** Encourage reporting of maritime threats within defined areas.

**Yaoundé Architecture for Maritime Security (YAMS)**



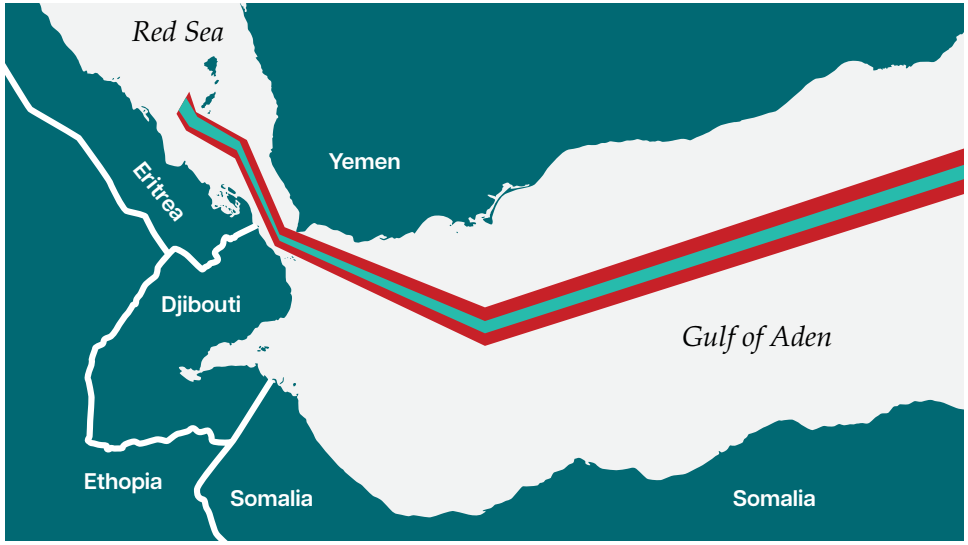
- **Benefit:** Provides data to improve regional maritime security and incident response.
- **Usage:** Ships should register and report their positions, suspicious activities and incidents.

Voluntary Reporting Areas (VRA) may be established in geographic areas where maritime threats to seafarers and ships is raised. Advice on their use together with reporting formats and instructions can be found on the security charts or the websites of regional reporting centres. The VRAs as shown on the charts clearly define an area, so companies and ships transiting, trading, or operating in these regions can join a trusted reporting scheme.

### Maritime Security Transit Corridors

Maritime Security Transit Corridors (MSTC) are recommended routes for shipping along which naval forces may focus their presence and surveillance efforts. MSTCs will be shown on the maritime security charts and published by reporting centres. The MSTC example below is shown on UKHO Chart Q6099 and consists of the Traffic Separation Scheme (TSS) West of the Hanish Islands, the Bab el Mandeb TSS and a two-way route directly connecting to the Internationally Recognised Transit Corridor (IRTC). The industry website has details of all routing advice.

**MSTC example that consists of the Traffic Separation Scheme (TSS) West of the Hanish Islands, the Bab el Mandeb TSS and a two-way route directly connecting to the Internationally Recommended Transit Corridor (IRTC)**




### Joint War Committee

- **Role:** Lists areas of perceived enhanced risk, affecting insurance premiums.
- **Listed areas:** lmalloyds.com/lma/jointwar

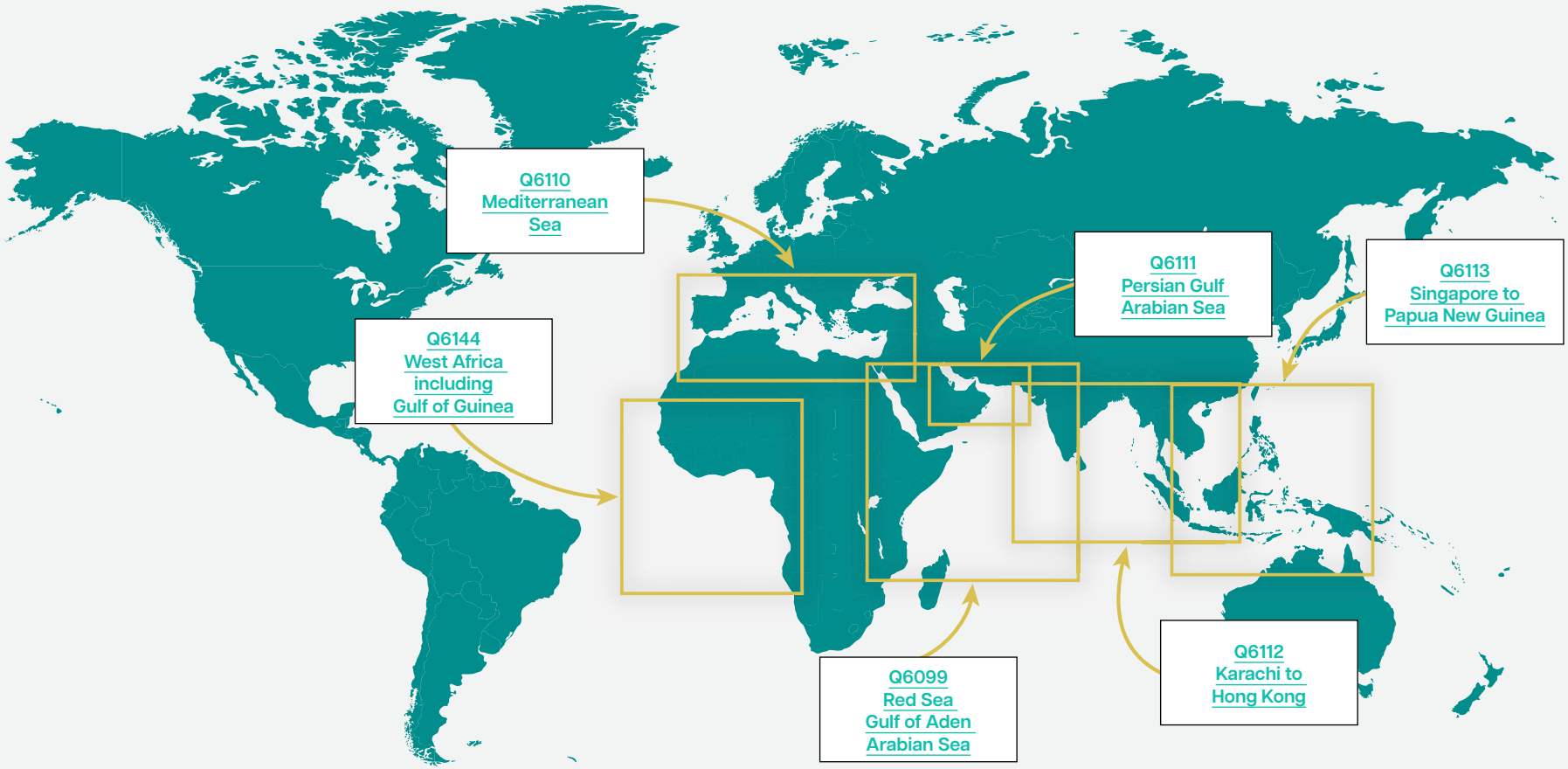
The insurance community may list an area of perceived enhanced risk in the region. Ships entering the area would need to notify their insurers and additional insurance premiums may apply. The Joint War Committee (JWC) comprises underwriting representatives from both Lloyd's and the International Underwriting Association representing the interests of those who write marine hull war business in the London market.

### Reporting suspicious activity

Seafarers play a crucial role in maritime security by reporting suspicious activities. Reports, including photographs, videos and radar data, are valuable to authorities.

Seafarers are encouraged to report any suspicious activity to the relevant global reporting centres to aid in improving maritime security and response. Typical suspicious activity is described in annex C.

## Limits of Maritime Security Charts





ANNEX B

# SEAFARER WELFARE SUPPORT

# Annex B – Seafarer welfare support

**Befrienders Worldwide (BW)** are very familiar with the unique realities of life at sea. If seafarers are missing home, fatigued from working long days, or experiencing a crisis, help is available. BW is a global charity with over 400 help centres across five continents, providing confidential, compassionate, and non-judgmental support – free of charge.

If you or someone you know needs support, go to:
Seafarer support:
befrienders.org/befrienders-worldwide-seafarers
Befrienders Worldwide: befrienders.org

**The International Christian Maritime Association (ICMA)** is a worldwide association of 27 Christian charities dedicated to the service of seafarers, fishers and their families. icma.as

**The International Seafarers' Welfare and Assistance Network (ISWAN)** is an international not for profit maritime organisation that works to improve the lives of seafarers and their families with services, resources, strategies and advocacy. ISWAN operates SeafarerHelp – a free, confidential, multilingual helpline for seafarers and their families. The service is available 24 hours a day, 365 days a year.

Phone: +44 (0)20 7323 2737 (request a call back): iswan.org.uk/get-support/seafarers/request-a-call-back/
Email: help@seafarerhelp.org
Live Chat: via iswan.org.uk/seafarerhelp
WhatsApp: +44 7909 470732
Facebook: facebook.com/seafarerhelp
SMS: +44 7860 018538
Skype: info-seafarerhelp.org
ВКонтакте: vk.com/seafarerhelpclub
Website: iswan.org.uk/seafarerhelp

The **Maritime Wellbeing** programme offers practical tips, tools and strategies for how to improve and raise awareness of mental and physical health. maritimewellbeing.com

**The Mission to Seafarers** is the largest provider of port-based welfare services, working in 200 ports across 50 countries supporting men and women working at sea. In addition, to their free services of Wi-fi, respite and transportation, their chaplains are trained in post-trauma counselling and are able to provide immediate support post attack or crew release, as well as connect with relevant professional services in the seafarers home country. There are two main email addresses for crew assistance: crewhelp@mtsmail.org and infomanila@missiontoseafarers.org – the latter being their Family Support Network in the Philippines.

**Sailors' Society** is a 200-year-old global maritime welfare charity supporting seafarers and their families in need, day and night, 365 days a year. Its international team of chaplains is always at the end of the phone or chat message to give comfort, advice on the charity's emergency grants and provide crisis response.

Their 24/7 Crisis Response Network and helpline provides care and support to seafarers, their families and shipping companies following critical incidents such as piracy, accident, and natural disasters.

The Society also offers seafarers a MyWellness e-learning app.sailors-society.org

**The Seafarers Hospital Society** is dedicated to maintaining the health, welfare and advice needs of seafarers of any nationality based in UK waters, and their families, through the provision of health and welfare grants. seahospital.org.uk

**Stella Maris** is the world's largest ship visiting charity with a global network of over 1,000 chaplains and volunteers based in 353 ports across 57 countries. Via its extensive network, and its Centenary Emergency Fund, Stella Maris provides timely, seamless, and focused support to seafarers, fishers and their families affected by abandonment, bereavement, conflicts, and other crises.
stellamaris.org.uk

ANNEX C

# MARITIME LEXICON AND ABBREVIATIONS

# Annex C – Maritime lexicon and abbreviations

## Maritime lexicon

The maritime industry will use the following lexicon to report/describe maritime security events, some of which are not covered by this publication.

### Maritime security threats

These threats often involve aggressive attackers who subject victims to violence and ill-treatment, hijack ships for ransom or cargo theft, and, in some cases, hold seafarer's hostage for extended periods. Attackers' motivations may be criminal, ideological or political, and attacks may be targeted or opportunistic. Maritime security threats vary across regions and within them both in terms of the threats themselves and their severity.

### Piracy

According to Article 101 of the UNCLOS, piracy includes:

- Any illegal act of violence, detention, or depredation committed for private ends by the crew or passengers of a private ship or aircraft, directed:
  - On the high seas, against another ship or persons or property onboard.
  - Against a ship, persons, or property in a place outside the jurisdiction of any state.
- Voluntary participation in operating a ship or aircraft with knowledge that it is a pirate vessel.
- Inciting or intentionally facilitating an act described above.

### Armed robbery against ships

As defined by the IMO Assembly Resolution A.1025(26), armed robbery against ships involves:

- Any illegal act of violence, detention, depredation, or threat thereof, committed for private ends and directed against a ship, or persons or property onboard, within a state's internal waters, archipelagic waters, and territorial sea.
- Inciting or intentionally facilitating such acts.

Maritime activity is diverse and sometimes the exact location of an incident is unavailable to correctly classify it. Hence, while capturing the incident, classification types used include:

- **Hijack:** attackers take control of a ship against the crew's will for purposes such as robbery, cargo theft, or kidnapping.
- **Kidnap:** unauthorised forcible removal of persons from the ship.
- **Attack:** aggressive approach with weapons discharged or missiles/loitering munitions hitting on or near the ship.
- **Illegal boarding:** boarding with intent to steal or harm without taking control.
  - **Sea theft:** stealing property without violence.
  - **Sea robbery:** stealing property with violence or use of arms.
- **Attempted boarding:** close approach with visible boarding paraphernalia, thwarted by defensive measures.
- **Suspicious activity:** unaccountable actions indicating potential threats, such as unusual equipment or behaviour. Indications may include:
  - The number of crew on board relative to its size.
  - The Closest Point of Approach.
  - The existence of unusual and non-fishing equipment on board, 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.

This is not an exhaustive list. Other events, activity and ships 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 among the maritime community.

## Abbreviations

| | |
|---|---|
| **AIS** | Automatic Identification System |
| **ALARP** | As Low as Reasonably Practicable |
| **ASM** | Anti-Ship Missile |
| **AWNIS** | Allied Worldwide Navigational Information System |
| **BAM** | Bab el Mandeb |
| **BMP** | Best Management Practice |
| **CCC** | Command and Coordination Centre |
| **CCTV** | Closed Circuit Television |
| **CMID** | Common Marine Inspection Document |
| **CMF** | Combined Maritime Forces |
| **CPA** | Closest Point of Approach |
| **CSO** | Company Security Officer |
| **DSC** | Digital Selective Calling |
| **ECDIS** | Electronic Chart Display and Information System |
| **ECP** | Emergency Communications Plan |
| **ECR** | Engine Control Room |
| **EU** | European Union |
| **EU MSC-IO** | European Union Maritime Security Center – Indian Ocean |
| **EUNAVFOR** | European Union Naval Force |
| **GNSS** | Global Navigation Satellite System |
| **GPS** | Global Positioning System |
| **GRP** | Glass Reinforced Plastic |
| **HOA** | Horn of Africa |
| **HQ** | Headquarters |
| **HSSE** | Health, Safety, Security and Environment |
| **IBF** | International Bargaining Forum |
| **IFC** | Information Fusion Centre |
| **IFC-IOR** | Information Fusion Centre – Indian Ocean Region |
| **IMB** | International Maritime Bureau |
| **IMO** | International Maritime Organization |
| **INTERPOL** | International Criminal Police Organisation |
| **IRTA** | Industry Releasable Threat Assessment |
| **IRTB** | Industry Releasable Threat Bulletin |
| **IRTC** | Internationally Recommended Transit Corridor |
| **ISC** | Information Sharing Center |
| **ISO** | International Organization for Standardization |
| **ISPS** | International Ship and Port Facility Security |
| **JISG** | Joint Industry Security Group |
| **JMIC** | Joint Maritime Information Center |
| **JWC** | Joint war Committee |
| **KFR** | Kidnap for Ransom |
| **LM** | Loitering Munitions |
| **LRIT** | Long-Range Identification and Tracking |
| **MDA** | Mine Danger Area |
| **MDAT-GOG** | Maritime Domain Awareness for Trade – Gulf of Guinea |
| **MMCC** | Maritime Multinational Coordination Centre |
| **MoU** | Memorandum of Understanding |
| **MSC** | Maritime Safety Committee |
| **MSTC** | Maritime Security Transit Corridor |
| **MTA** | Mine Threat Area |

| | |
|---|---|
| **NATO** | North Atlantic Treaty Organisation |
| **NAVAREA** | Navigation Area |
| **NCAGS** | Naval Cooperation and Guidance for Shipping |
| **NSC** | NATO Shipping Centre |
| **OOW** | Officer of the Watch |
| **OVID** | Offshore Vessel Inspection Database |
| **P&I** | Protection and Indemnity |
| **PA** | Public Address |
| **PAG** | Pirate Action Group |
| **PAST** | Private Armed Security Teams |
| **PCASP** | Privately Contracted Armed Security Personnel |
| **PMSC** | Private Maritime Security Company |
| **PPE** | Personal Protective Equipment |
| **RECAAP** | Regional Cooperation Agreement on Combating Piracy & Armed Robbery against Ships in Asia |
| **ROE** | Rules of Engagement |
| **RPG** | Rocket Propelled Grenade |
| **RUF** | Rules for the Use of Force |
| **RV** | Rendezvous |
| **SATCOM** | Satellite Communications |
| **SBM** | Single Buoy Mooring |
| **SEV** | Security Escort Vessel |
| **SOH** | Straits of Hormuz |
| **SOLAS** | Safety of Life at Sea |
| **SPM** | Ship Protection Measures |
| **SSA** | Ship Security Assessment |
| **SSAS** | Ship Security Alert System |
| **SSO** | Ship Security Officer |
| **SSP** | Ship Security Plan |
| **STS** | Ship to Ship |
| **TSS** | Traffic Separation Scheme |
| **UAV** | Unmanned Aerial Vehicle |
| **UKHO** | United Kingdom Hydrographic Office |
| **UKMTO** | United Kingdom Maritime Trade Operations |
| **UNCLOS** | United Nations Convention on the Law of the Sea |
| **USV** | Uncrewed Surface Vehicle |
| **UUV** | Unmanned Underwater Vehicle |
| **UXO** | Unexploded Ordnance |
| **VDR** | Voyage Data Recorder |
| **VHF** | Very High Frequency |
| **VHP** | Vessel Hardening Plan |
| **VMS** | Vessel Monitoring System |
| **VPD** | Vessel Protection Detachment |
| **VRA** | Voluntary Reporting Area |
| **WBIED** | Water-Borne Improvised Explosive Devices |