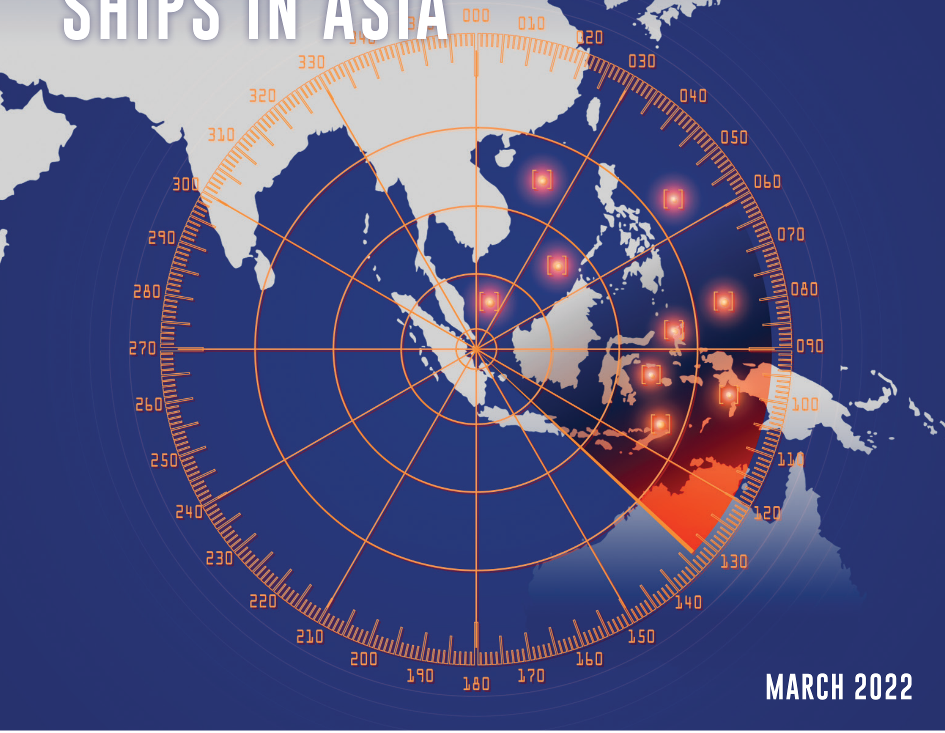
REGIONAL GUIDE 2
TO COUNTER PIRACY AND ARMED ROBBERY AGAINST SHIPS IN ASIA



MARCH 2022

Working Group:

ReCAAP Information Sharing Centre

INFORMATION FUSION CENTRE

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

ASA Asian Shipowners' Association

FEDERATION OF ASEAN SHIPOWNERS' ASSOCIATIONS

INTERTANKO

OCIMF

SSA SINGAPORE SHIPPING ASSOCIATION

ACKNOWLEDGEMENT

This guide was produced by the ReCAAP ISC in collaboration with the Asian Shipowners' Association (ASA), Federation of ASEAN Shipowners' Associations (FASA), Information Fusion Centre (IFC), INTERTANKO, Oil Companies International Marine Forum (OCIMF), S. Rajaratnam School of International Studies (RSIS) and Singapore Shipping Association (SSA), in the desire to promote safe and secure seas for the shipping community. The authors also acknowledge the use of BMP5 in the production of this guide.

DISCLAIMER

This Guide, compiled for the Asian region, has been prepared for general advisory purpose. This Guide does not and shall not be construed to impose any obligation or requirement on ship owners or managers to implement any of the measures or advice therein, and any person or entity who wishes to implement the same is advised to exercise due care and discretion in doing so, having due regard to their own requirements and resource capabilities. Further, whilst due care and diligence has been exercised by the publishers, authors, their employers, employees and all persons or entities involved in the preparation, publication, supply, and dissemination of this Guide is provided without any representation or warranty whatsoever, including any as to its suitability for implementation by any person or entity.

CONTENTS

THE FUNDAMENTAL REQUIREMENTS OF THIS GUIDANCE

Understand the threat

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

Conduct risk assessments

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

Implement ship protection measures

- Harden the ship.
- Brief and train the crew.
- Enhanced lookout.
- Follow flag State, insurance and regional guidance.

Report

- Register and report to Regional Centres.
- Report incidents and suspicious activities to coastal States and Regional Centres.
- Send distress signal when attacked.

Cooperate

- Cooperate with coastal States.
- Cooperate with law enforcement to preserve evidence.
- Cooperate with welfare providers.

SECTION 1
INTRODUCTION

Piracy and armed robbery against ships in the Asian region has evolved over the years. In recent years, the perpetrators usually board ships to steal unsecured items, ship stores and engine spares.   They do not confront and harm the crew in most cases. Most of the incidents in the Asian region are different from those in the African region (waters off Somalia, the Gulf of Aden, the Gulf of Guinea) where, in many cases, the crew are kidnapped for ransom or treated with violence.

However, the number of incidents in Asia is still higher than in other regions of the world. Even without confrontation, unauthorised boarding poses a threat and violence to the seafarers and safety of navigation. There are also some serious incidents involving violence against the crew in Asia as well. These incidents are often committed by organised criminal groups and can include hijackings of tug boats and barges for resale, oil cargo theft from tankers, and abduction of crew for ransom.

In the past 15-years (2007-2021), 81% of the incidents were armed robbery against ships, and 19% were piracy incidents. This meant that most of the incidents occurred in the territorial seas/archipelagic waters where the coastal States have the jurisdiction and responsibility to enforce the law. However, for incidents of piracy which occur beyond the territorial seas/ archipelagic waters, all States can intervene and arrest the pirates[1].

In response to the increase in incidents involving hijacking of tug boats and barges between 2008 and 2012, the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia Information Sharing Centre (ReCAAP ISC) launched the *Tug Boats and Barges (TaB) Guide Against Piracy and Sea Robbery* in January 2013. A spike in the number of incidents involving theft of oil cargo from tankers in 2014 and 2015 led to the release of the *Guide for Tankers Operating in Asia against Piracy and Armed Robbery Involving Oil Cargo Theft* in November 2015.

[1] The definition of 'piracy' in accordance with the United Nations Convention on the Law of the Sea (UNCLOS), and 'armed robbery against ships' in accordance with the International Maritime Organisation (IMO) Assembly Resolution A. 1025 (26) Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery Against Ships. The detailed definitions are in **Annex A**.

The maritime community’s request for a comprehensive guide which covers all types of ship operating in Asian waters prompted the production of the *Regional Guide to Counter Piracy and Armed Robbery Against Ships in Asia*. Launched in February 2016, the Regional Guide encompasses the two earlier guides mentioned and takes into consideration the incidents involving all types of ship underway and at ports and anchorages in Asian waters.

Incidents of crew abduction for ransom by the Abu Sayyaf Group (ASG) in the Sulu-Celebes Seas were first reported in March 2016, after this Guide was published. In response to the incidents of crew abduction, the *Guidance on Abduction of Crew in the Sulu-Celebes Seas and waters off Eastern Sabah* was produced in July 2019.

This Regional Guide (Version 2) includes updated information such as the modus operandi for the different types of perpetrators and contact details of the relevant agencies. It is designed to assist the Owner/Operator/ Master and crew operating in Asia to adopt the appropriate measures to avoid, deter or delay attacks and unauthorised boardings. This Guide complements information provided by the IMO, particularly the reporting of incidents to the nearest coastal State and flag State as stipulated in the MSC.1 Circular 1333/Rev.1 and Circular 1334 (refer to **Annex B** of this Guide). This Guide should be read with the latest information and assessment of the situation in the reports issued by the ReCAAP ISC (https://www.recaap.org), Information Fusion Centre (IFC) (https://www.ifc.org.sg) and the International Maritime Bureau (IMB) (https://www.icc-ccs.org/icc/imb) whose contact details can be found in **Annex D**.

SECTION 2
GEOGRAPHICAL LOCATION

The Asian region in this Guide refers to the geographical limits of the areas of responsibility of the countries as stated in Article 18 (1) of the ReCAAP Agreement — the waters surrounding Northeast Asia, Southeast Asia and South Asia.

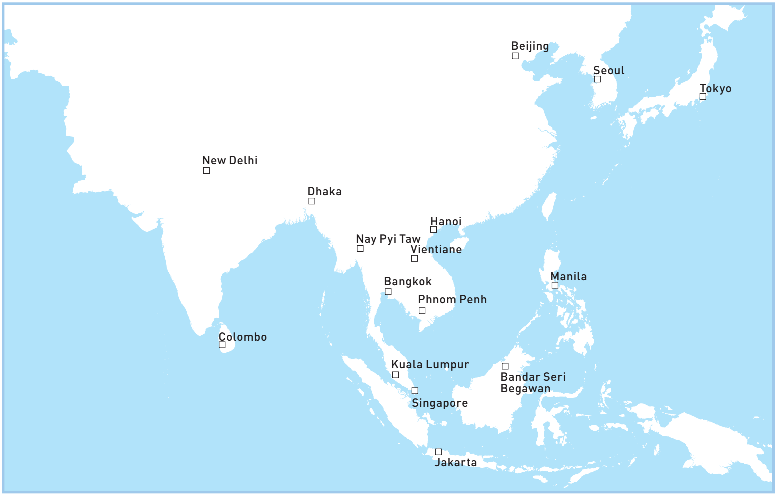


Figure 1: ReCAAP's geographical areas of responsibility

Since the establishment of the ReCAAP ISC in 2006, the locations and modus operandi of piracy and armed robbery against ships in Asia have evolved. In the past, most of the incidents occurred at ports and anchorages in Bangladesh, India, Indonesia, Malaysia, the Philippines and Vietnam; against ships underway in the Straits of Malacca and Singapore (SOMS), and against ships underway/anchored in the South China Sea. In 2020, most of the incidents occurred on board ships while underway in the Singapore Strait (SS) (primarily in the eastbound lane of the Traffic Separation Scheme [TSS]), and on board ships berthed/anchored in Bangladesh, India, Indonesia, the Philippines and Vietnam. In 2021, incidents continued to occur in the SS, while the number of incidents in the other locations in Asia has decreased.

During 2014 and 2015, the incidents of oil cargo theft committed by organised criminal groups occurred mostly in the southern region of the South China Sea and in the Malacca Strait. Although there has been no report of such incidents since 2016, the risk still remains. From March 2016, there have been incidents of abduction of crew by the ASG in the Sulu-Celebes Seas and waters off Eastern Sabah with the last reported incident occurring in January 2020. Despite the pause, the risk of abduction of crew in that area remains high because the active members of the ASG remain at large.

It is strongly advised to refer to ReCAAP ISC, IFC and IMB for updates on the latest situation and areas of concern. Refer to **Annex D** for their contact details.

SECTION 3
THREATS AND MODUS OPERANDI

The current threats in Asia, at the time of this publication, are armed robbery and theft along the eastbound lane of the SS and at some ports and anchorages as well as abduction of crew for ransom off Eastern Sabah (Malaysia) and in the Sulu-Celebes Seas (Philippines). There have been also more serious incidents such as the hijacking of tug boats and barges for resale, and hijacking of small tankers for oil cargo theft. Such incidents are committed by organised criminal groups and very often involved violence against the crew. The key Modus Operandi are highlighted in the following paragraphs.

A. UNDERWAY

The criminal activities involving ships underway in the Asian region can be broadly grouped into the following categories:

Armed robbery and theft – In general, such activities are opportunistic in nature and occur when ships are in coastal waters. Ships are particularly vulnerable when the bridge team is involved in navigating through congested waters and island groups. Incidents on board ships underway have occurred in the SOMS, particularly in the eastbound lane of the TSS in the SS, and in the South China Sea. The perpetrators' primary aim is to steal and escape without being sighted by the crew.

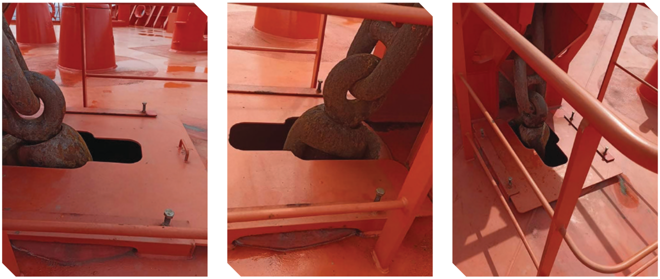
Hijacking of ships – At the time of publication, the last hijack reported in Asia happened in May 2016. This incident involving an oil tanker in Southeast Asian waters. Hijackings of tankers normally occurs during hours of darkness; and have occurred primarily in the southern region of the South China Sea, and in the Malacca Strait from 2011 to 2017. These attacks have been restricted to small tankers especially those with low freeboard. While there has been no reported hijacking of ships since 2017, small and large tankers are advised to take precautionary measures. Ships transporting specific grade of oil cargo have been targeted, suggesting the perpetrators receive insider information on the cargo, schedule and route of the targeted ships. Ships could be hijacked for several hours or days for oil cargo to be transferred to a smaller "feeder" ship. There have been cases where the identities of the ships were 'disguised' and the crew were left adrift in lifeboats or left ashore in remote areas. The other type of hijacking that have occurred in Asian waters from 2007 to 2014 have been the theft of tug boats and other smaller ships for black market resale.

Abduction of crew for ransom – Serious crimes of abduction of crew for ransom carried out by the ASG occurred on board ships transiting the waters off Eastern Sabah, Malaysia and in the Sulu-Celebes Seas in the Philippines. They usually target slow-moving and low freeboard ships such as tug boats and fishing boats/trawlers. They have also attempted to attack larger ships, but without success. The objective of the perpetrators was to demand ransom money from the ship owners or relatives of the abducted victims. Due to the efforts of the Philippine and Malaysian authorities, sub-leaders and members of abduction group have been neutralised or arrested and, at the time of publication, the last incident of abduction of crew occurred in January 2020. However, the risk of abduction of crew in the area remains high as some members of the abduction group are still at large.

Method and equipment used for boarding – In Asia, the perpetrators often use wooden small boats or fishing boats (to avoid being noticed) and a variety of tools including poles, hooks and lines to board ships. The use of a mothership is not common in Asia as most of the incidents occur within ports and anchorages or in coastal areas. Even for piracy incidents on high seas, mostly in the South China Sea, the use of a mothership is not common due to the relatively short distance from the shore.

B. PORTS, ANCHORAGES AND SHIP TO SHIP (STS) TRANSFERS

At certain ports and anchorages, the risk of armed robbery and theft is higher when the ship is at anchor or is drifting off port (when approaching the pilot station or conducting STS operation). When alongside at port and anchorage or during STS operation, equipment such as fenders, anchor chains, and hawse pipes should be physically blocked as they can provide a vulnerable point of access for perpetrators. The perpetrators often use fishing boats to approach the victim ship. Particular attention should be paid to suspicious small boats passing close to a ship or loitering in the vicinity. The perpetrators usually board ships during hours of darkness to avoid being detected.



Sealed anchor chain hawse pipe hole
[Courtesy of ReCAAP Focal Point (Philippines)]

STS Operations

The following precautionary measures should be taken during STS operations:

- Change the location of STS (if operations permit) to avoid predictable patterns which can be exploited by criminals.
- Conduct STS transfer operations during daylight hours, when possible.
- Ship operators should consider what security measures the STS Service provider has in place for the operation. The Risk Assessment of the company providing the STS Service should be reviewed by the Ship Security Officer (SSO) and the ship's Master. Refer to Section 4 on 'Threat and Risk Assessment'.
- When STS operations are expected to be conducted, extra attention should be paid to the use of physical protection measures. As razor wire can potentially make it very difficult to complete STS operations, other protective measures should be considered to protect the ship from unauthorised boarding.

Please refer to BMP West Africa for '*Security measures for Floating (Production) Storage & Offloading (F(P)SO)*' (https://www.maritimeglobalsecurity.org/media/1048/bmp-wa-lo-res.pdf).

SECTION 4
THREAT AND RISK ASSESSMENT

A Risk Assessment is a logical examination of the current situation to identify the threats likely to be encountered. It should examine the effectiveness of the security measures already in place and identify additional prevention, mitigation and recovery measures available. A Risk Assessment must be ship-specific and voyage-specific and should be carried out prior to entering the sea areas described in Section 3.

The Risk Assessment should include, but not be limited to, the following:

- Crew safety (measures to prevent illegal boarding and external access to accommodation space, whilst ensuring that the crew will not be trapped inside and will be able to escape in the event of a fire, flooding, or other emergency)
- The specific threat (who are likely the pirates/armed robbers, what do they want to achieve, how do they attack, how do they board, which weapons do they use etc). The latest on the threat situation may be obtained from the ReCAAP ISC, IFC, regional reporting centres, shipping associations, IMB, commercial intelligence providers or local sources e.g. ships' agents.
- The ship's and company's procedures (drills, watch rosters, chain of command, decision making processes, etc.).
- Background factors that may affect the unauthorised boarding (geography, visibility, sea-state, speed, wind, weather, swell, wave height, traffic density, and local patterns of activity, for example, other commercial ships, fishing concentration areas, etc.)
- The ship's characteristics/vulnerabilities/inherent capabilities to deal with the threat (for example, ship's freeboard, speed, general arrangement, etc.)
- Ship's procedures (such as drills, watch rotation, routine maintenance, etc.)
- Planning and procedures (time/duration/season of transit – day/night)
- Any statutory requirements, in particular those of the flag State and or the coastal and port State. Other requirements dictated by the company, charterer, and insurance policies should also be taken into consideration.

The Risk Assessment Process

The risk being evaluated is the likelihood of harm to the crew or ship from a maritime security threat. Risk Assessment must reflect the prevailing characteristics of the specific voyage and ship and not just be a repetition of advice relating to a different geographical region and a different modus operandi of the perpetrators. Detailed guidance on preparing risk assessments can be found from a variety of sources including the International Ship and Port Facility Security (ISPS) code.

Record of the Risk Assessment

Records of the risk assessment should be maintained by the Company Security Officer (CSO) and the crew on board the ship. These should be reviewed and updated on a regular basis to capture lessons learned and identify gaps. This will generate improvements and provide examples of best practices. These risk assessments can be used to educate staff and serve as training aids for staff and crew. As more people read and understand the risk assessment, the level of preparedness and the likelihood of spotting omissions and suggesting improvements would increase. The protection measures identified in the risk assessment process should be recorded on the ship specific hardening plan for reference in conjunction with the current voyages risk assessment.

Self-Protection Measures

When the threat level is elevated either by prior warning, intelligence, information from the regional reporting centres or threat detection, additional control measures need to be predefined and applied to reduce the risk to an acceptable level. This is elaborated in Section 7 of this Guide.

SECTION 5
COMPANY PLANNING

It is strongly recommended that ship owners and operators adopt the following company planning procedures when operating in the region. Prior to entering the area:

- **Review the threat and risk assessment with the Master**.
- **Obtain the latest information from the ReCAAP ISC, IFC, IMB, IMO, and other relevant regional agencies**. Great care should be taken in voyage planning given the difficulty in predicting an area where a ship might fall victim to piracy or armed robbery. Information from shipping associations, commercial intelligence providers, or local sources may be useful for voyage planning.
- **Review the Ship Security Assessment (SSA), Ship Security Plan (SSP) and Vessel Hardening Plan (VHP)**. Review the SSA and implementation of the SSP, as required by the ISPS Code.
- **Monitor piracy-related websites on specific threats**. Ensure that ships are aware of any specific threats that have been promulgated.
- **Provide guidance to Master with regard to the recommended route**. Provide guidance to the Master with regard to the recommended route through the area of concern and details of the potential threat.
- **Plan and install Ship Protection Measures**. The provision of carefully planned and installed Ship Protection Measures prior to transiting an area of concern is strongly recommended. Suggested Ship Protection Measures are set out within this Guide – see Section 7. It has been proven that the use of Ship Protection Measures significantly increases the prospects of a ship resisting an attack.
- **Tracking**. Ship owners should consider the placement of hidden position transmitting devices, as one of the first actions of hijackers is to disable all visible communication systems, tracking devices, and aerials.
- **Conduct crew training**. Conduct crew training sessions (including citadel drills when utilised) prior to transits with ship protection measures in place.
- **Obtain contact details**. Ensure that contact details of the nearest coastal States are readily available and easily accessible. Refer to **Annex D**.

- **Participate in the Voluntary Community Reporting (VCR) scheme**. It is strongly recommended that ship operators register with IFC before entering the VCR area. Refer to Section 8.
- **Review manning requirements**. Consider disembarking non-essential crew.

Information Security:

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

- Communications with external parties should be kept to a minimum, with close attention paid to organising rendezvous points and waiting positions.
- Email correspondence to agents, charterers and chandlers should be controlled and information within the email kept concise, containing the minimum that is contractually required.
- If the ship trades regularly in the region, it is recommended to make varied arrangements whenever possible to make it difficult for criminals to predict where operations or voyage might take place.

Private Maritime Security Contractors (PMSCs).

Privately Contracted Armed Security Personnel (PCASP) are prohibited by law from operating inside territorial waters of most of the coastal States in Asia. The authorities are enforcing these regulations vigorously.

Unarmed PMSCs are a matter for individual ship operators following their own voyage risk assessment. Companies are advised to check the laws and regulations of flag States and coastal/port States in Asia concerning PMSC (particularly PCASP) so as not to violate applicable laws and regulations.

SECTION 6
MASTER PLANNING

It is recommended that ship Masters plan according to the following prior to entering an area of concern:

- **Review risk assessment**. The Master (and Company) should appreciate that the voyage routing may need to be reviewed in light of updated information received. Given the modus operandi of the perpetrators operating in Asia, the Master should plan with the following in mind:

    - Where possible, drifting, waiting and slow steaming should be avoided.
    - Where practicable, a prolonged stay at an anchorage is to be avoided. Anchoring within a designated anchorage area is strongly encouraged as it deters unauthorised boarding.
    - Minimize use of Very High Frequency (VHF) radio. Instead, use e-mail or secure satellite telephone. Where possible, only answer known or legitimate callers on the VHF, bearing in mind that the callers may be imposters.
    - Most incidents of piracy and armed robbery have occurred during hours of darkness. Where possible, plan operations to start and end during daylight hours.
    - Maintain constant radio watch and communication with CSO.
    - Listen to the latest Navigational Area (NAVAREA) warnings and alerts.
    - Heighten alertness and enhance vigilance during passage through areas of concern.

- **Brief crew and conduct drill.** Prior to entry into an area of concern, it is recommended that the crew should be fully briefed on the preparations and a drill conducted with the ship protection measures in place. The plan should be reviewed and all personnel briefed on their duties, including familiarity with the alarm which signals an attack, an all-clear situation, and the appropriate response to each. The drill should also consider the following (next page):

  - Testing the ship's protection measures, including testing of the security of all access points.
  - A thorough review of the SSP and VHP (see Section 5).
  - Lock-down conditions, including crew safety considerations.
  - Passage plan should incorporate security considerations.
  - Guidance to the bridge team on vigilance should be stated in night orders.

- **Prepare and Test of Emergency Communication Plan**. Masters are advised to prepare an Emergency Communication Plan. This should include all essential emergency contact numbers and prepared messages. It should be ready at hand or permanently displayed near all external communications stations including the safe muster point or citadel (see list of Contacts in **Annex D**). Communication devices and the Ship Security Alert System (SSAS) should be tested.

- **Discretion of the activation of the ship's Automatic Identification System (AIS) policy**. It is recommended that the AIS remains switched on at all times. However, Masters have the discretion to switch off the AIS if he believes that its use increases the ship's vulnerability. It is recommended that in an area of concern, AIS status be restricted to the ship's identity, position, course, speed, navigational status, and safety-related information.

Upon entering an area of concern:

- **Keep maintenance and engineering work to a minimum**:

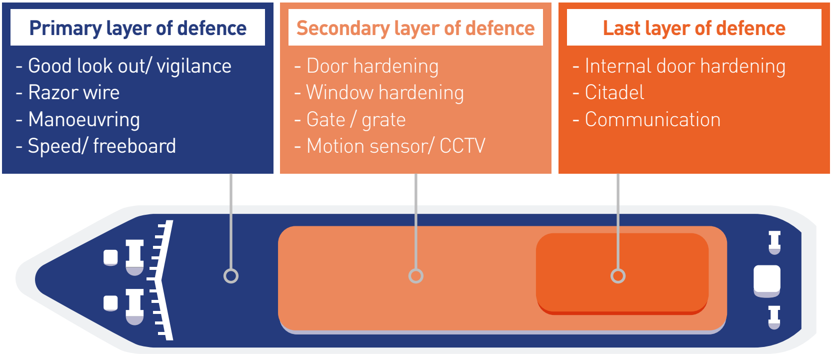
  - Ensure all access points are limited and controlled.
  - All essential equipment should be readily available – appropriate consideration on risk should be given when considering maintenance on essential equipment.
  - All cutting equipment should be stowed and secured from access.

SECTION 7
SHIP PROTECTION MEASURES

The guidance within this section primarily focuses on preparations that might be within the capability of the ship's crew or be feasible with some external assistance.

The guidance is based on regional experiences and may require change if the perpetrators alter their modus operandi.

The Ship Protection Measures described in this section have been effective, however, layered protection is recommended to help deter and delay unauthorised boarding.



Primary layer of defence

- Good look out/ vigilance
- Razor wire
- Manoeuvring
- Speed/ freeboard

Secondary layer of defence

- Door hardening
- Window hardening
- Gate / grate
- Motion sensor/ CCTV

Last layer of defence

- Internal door hardening
- Citadel
- Communication

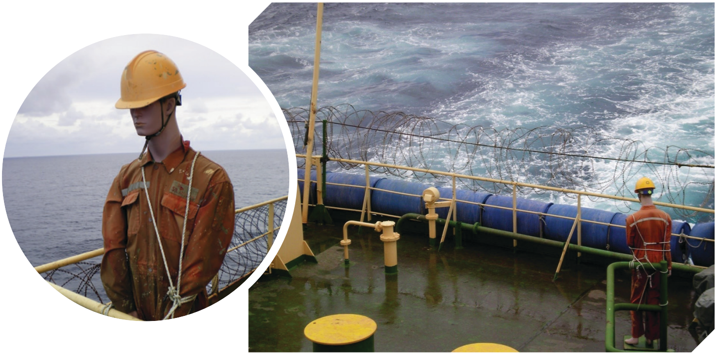
Figure 2: Example of layered protection

Ship owners may wish to consider making further alterations to the ship beyond the scope of this Guide, and/or provide additional equipment and/ or manpower as a means of further reducing the risk of unauthorised boarding. If perpetrators are unable to board a ship, they cannot hijack it, neither can they steal anything from the ship nor harm the crew.

Watchkeeping and Enhanced Vigilance

Prior to entering an area of concern, it is recommended that preparations as directed by the risk assessment are made:

- Consider a shorter rotation of the watch period in order to maximise alertness of the lookouts, and ensure that lookouts are fully briefed and trained.
- Ensure that there are sufficient binoculars for the enhanced Bridge Team, preferably the anti-glare type.
- Consider the use of thermal imagery optics and night vision aids.
- Maintain a careful radar watch.
- Watch for approaching small ships from the stern.
- Consider enhancing technology where possible, such as installing Closed Circuit Television (CCTV).
- Whilst underway, consider the use of downward facing lighting around the stern. The ship search light has also proved to be effective in enhancing the lookout for any suspicious ships approaching the stern.



Courtesy of Korean Shipping Association (KSA)

Enhanced Bridge Protection

The bridge is usually the focus of any attack. If the perpetrators are able to board the ship, they usually go to the bridge to gain control of the ship. The following enhanced protection measures should be considered:

- While most bridge windows are laminated, further protection against flying glass can be provided by the application of security glass film, often called Blast Resistant Film.
- Use fabricated metal (steel/aluminium), for hardening the side and rear bridge windows and the bridge wing door windows, (for example, consider metal grills or window bars) which may be permanently installed or rapidly secured in the event of an unauthorised boarding.

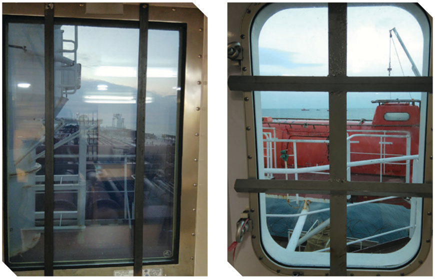
Courtesy of IFC

Courtesy of ReCAAP Focal Point (Thailand)

Control of Access to Bridge, Accommodation, and Machinery Spaces

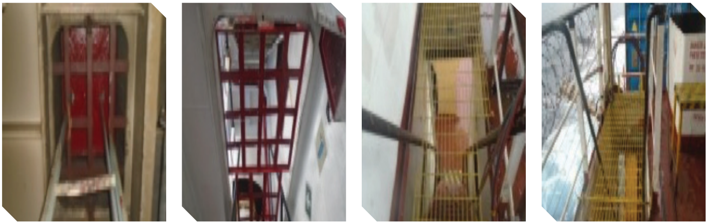
- It is very important to control the access routes to further deter or delay perpetrators who manage to board a ship and try to enter the accommodation or machinery spaces. If the perpetrators manage to gain access to the upper deck of a ship, they will generally be tenacious in their efforts to gain access to the accommodation section and, in particular, the bridge. It is strongly recommended that significant effort is expended to deny perpetrators' access to the accommodation and the bridge. However, escape routes must be easily accessible to the crew in the event of an emergency.

    - All doors and hatches providing access to the bridge, accommodation, and machinery spaces should be properly secured.



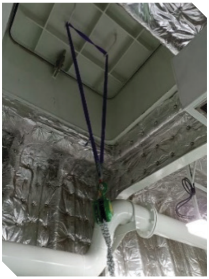
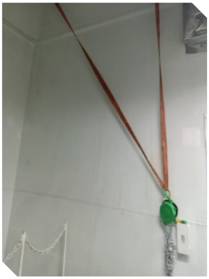
Courtesy of ReCAAP Focal Point (India)

    - Careful consideration should be given to the means of securing doors and hatches in order to provide maximum protection to the ship.
    - Consider installing gates/grates on external stairways.



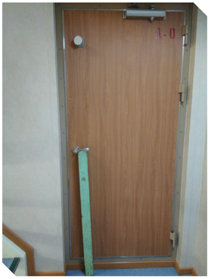
Courtesy of IFC

- Where the door or hatch is located on an escape route from a manned compartment, it is essential that it can be opened quickly and easily by a crew member trying to exit by that route. Where the door or hatch is locked it is essential that a key is available, in a clearly visible position by the door or hatch.

(Left) Courtesy of ReCAAP Focal Point (India)
(Middle & right) Courtesy of ReCAAP Focal Point (Philippines)

- It is recommended that once doors and hatches are secured, only designated doors and a limited number of them are used for routine access when required, with their use being strictly controlled
- Where doors and hatches are required to be closed for watertight integrity, ensure all clips are fully dogged down in addition to any locks. Where possible, additional securing, such as the use of wire strops, may enhance hatch security.
- Internal door hardening on the bridge has proven to be effective in allowing the bridge team more time to make their way to the citadel or Safe Muster Point.



(Left) Courtesy of ReCAAP Focal Point (Philippines)
(Right) Courtesy of ReCAAP Focal Point (India)

- Perpetrators have been known to gain access through portholes and windows. The fitting of steel bars to windows will deter and delay this even if they manage to shatter the window. Due consideration should be given for windows that are emergency escapes.
- Prior to entering the area of concern, procedures for controlling access to accommodation spaces, machinery spaces, and store rooms should be set out and practised.
- Ensure that tools on deck are properly stored and secured.

Courtesy of IFC

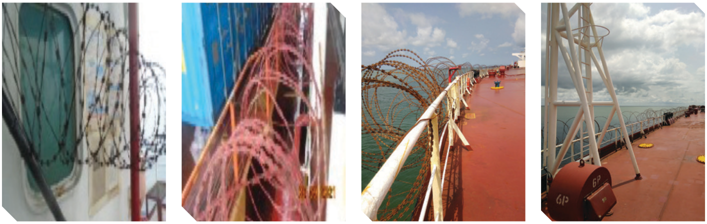
Physical Barriers

Perpetrators typically use long lightweight hooked ladders, grappling hooks with rope attached, and/or long hooked poles with a climbing rope attached to board ships while underway. Physical barriers should be used to make it as difficult as possible to gain access to the ship.

Before constructing any physical barriers, it is recommended that a thorough survey is conducted to identify areas vulnerable to perpetrators trying to gain access. Razor wire, gates, barriers, fences, or their combination have proved to be effective to prevent or delay unauthorized boarding. Due consideration should also be given to the safety of the crew in the event of an emergency.

Razor Wire

When deploying razor wire, personal protective equipment to protect hands, arms, and faces must be used. Moving razor wire using wire hooks (like meat hooks) rather than by gloved hand reduces the risk of injury. It is recommended that razor wire is provided in shorter sections (e.g. 10 metres per section) as it is significantly easier and safer to use than larger sections which can be very heavy and unwieldy.



(1st & 2nd photo from left) Courtesy of IFC
(1st & 2nd photo from right) Courtesy of ReCAAP Focal Point (India)

- A robust razor wire barrier is particularly effective if it is:
  - Constructed outboard of the ship's structure (i.e. overhanging) to make it more difficult for perpetrators to hook on their boarding ladder/grappling hooks to the ship's structure.
  - Constructed of a double roll of concertina wire around the proximity of the ship - some ships use a treble roll of concertina razor wire which is even more effective.
  - Constructed using high tensile concertina razor wire with coil diameters of 730mm or 980mm which is difficult to cut with hand tools.
  - When rigging razor wire care must be taken not to overstretch the wire in order to reduce the amount used. Doing so can make it ineffective.
- It is recommended that when rigging razor wire, a steel cable is run through the centre in order to offer additional strength and reduce a hostile attacker's ability to pull it down. The added advantage of having the steel cable is the ease of rigging and removal. This is particularly useful for ships operating on short voyages.
- Razor wire is most effective when rigged around the full proximity of the ship with a minimum of two layers, but this may not be ideal for all ships. An alternate solution would be to consider using razor wire in front of the accommodation in at least three layers in order to delay or deter attackers. If this method is adopted, due consideration should be given to the security of deck stores and the equipment forward of the barrier.

Water Spray and Foam Monitors

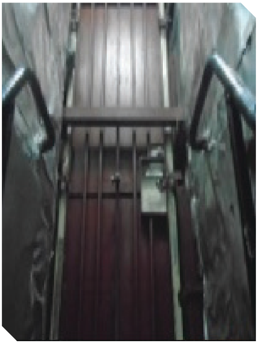
The use of water spray (such as from fire hoses) can make it difficult for a suspicious boat to remain alongside and makes it significantly more difficult for a perpetrator to climb on board.

- It is recommended hoses and foam monitors (delivering water) are fixed in position to cover likely access routes and are remotely operated. Manual activation is not recommended as this may place the operator in an exposed position.
- Improved water coverage may be achieved by using fire hoses in jet mode and using baffle plates fixed a short distance in front of the nozzle.
- Water cannons deliver water in a vertical sweeping arc and protect a greater part of the hull.
- Water spray rails with spray nozzles produce a water curtain covering larger areas.
- Foam can be used, but it must be in addition to a ship's standard fire fighting equipment stock. Foam is disorientating and very slippery.
- The use of all available fire and general service pumps may be required to ensure all defences operate efficiently.
- Additional power may be required when using pumps; the supporting systems should be ready for immediate use.
- Practice, observation and drills are required to ensure the equipment provides effective coverage of vulnerable areas.

Courtesy of ReCAAP Focal Point (Thailand)

Gates

An alternative option to secure the superstructure from a hostile attacker can be by means of a gate system securely rigged on the main deck in conjunction with accessible window hardening. This configuration will not only provide substantial protection but will also enable quick hardening of the ship's perimeter. However, gates should be used in conjunction with razor wires to prevent perpetrators going around the sides or climbing above the gates which are in place. Again, this will help protect the accommodation. If this method is adopted, due consideration should be given to the security of deck stores and the equipment forward of the barrier.



Courtesy of IFC

Alarms

When operating in an area of concern, procedures should be in place to ensure that the crew muster in a safe location and the crew are aware about the nature of the emergency.

Sounding the ship's alarms/whistle serves to inform the ship's crew that an attack has commenced and, importantly, demonstrates to any potential attacker that the ship is aware of the attack and is reacting. If approached, continuous sounding of the ship's foghorn/whistle can distract the perpetrators and as mentioned above lets them know that they have been detected. It is important to (next page):

- Sound the emergency alarm and announce that the ship is under attack.
- Conduct exercises prior to entering the area of concern.
- The alarms are distinctive to avoid confusion.
- Crew members are familiar with each alarm, especially those warning of an attack and indicating 'all clear'.
- All alarms are backed up by an announcement over the accommodation and deck PA system, where fitted.
- Drills are carried out to ensure that the alarm is heard throughout the ship. The drill will confirm the time necessary for all crew to move to a position of safety.

Manoeuvring Practice

Where navigationally safe to do so, ship Masters are encouraged to practise manoeuvring their ships to establish which series of helm orders produce the most difficult sea conditions to disrupt a perpetrator's boat from getting close enough to board the ship, without causing a significant reduction in the ship's speed.

CCTV

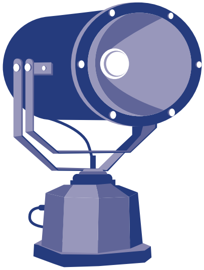
CCTV is not a substitute for a physical lookout. However:

- Consider the use of CCTV cameras to ensure coverage of vulnerable areas.
- Consider positioning CCTV monitors in a protected position.
- CCTV monitors could be located at the safe muster point/citadel and engine control room.
- Recorded CCTV footage may provide useful evidence after an attack.

Lighting

It is recommended that the following lights are made available and tested:

- Weather deck lighting around the accommodation block and rear-facing lighting on the poop deck, consistent with Rule 20(b) of the International Regulations for Preventing Collision at Sea.
- Search lights for immediate use when required.
- At anchorage, it is recommended that deck lightings be kept on as opportunistic boarding are less likely on well-lit ships. In compliance with international regulations, navigation lights should not be switched off at night.
- Once attackers have been identified or an attack commences, over side lighting, if fitted, should be switched on. This will dazzle the attackers and help the ship's crew to see them.
- The ability to turn off all internal accommodation lights to deter pirates from entering or disorientate those who may already have entered.



Deny Use of Ship's Tools and Equipment

Perpetrators generally board ships with little equipment other than their personal weaponry. It is important to try to deny them the use of ship's tools or equipment that may be used to gain entry into the ship. Tools and equipment, particularly cutting equipment, that may be of use to the perpetrators should be stored in a secured location.

Safe Muster Points and/or Citadels

Any decision to evacuate the bridge in congested waters when the ship's security is threatened requires careful consideration. Consideration must be given to establishing a safe muster point. Consideration should also be given to establishing a citadel. The company risk assessment and planning process should identify the location of a safe muster point and/or a citadel within a ship. An explanation of each is as follows (next page):

Safe Muster Point

A safe muster point is a designated area chosen to provide maximum physical protection to the crew, preferably lower down within the ship. The designated muster point should not be on the bridge.

In the event of a suspicious approach, crew not required on the Bridge or the Engine Room Control Room should muster at the safe muster point.

- A safe muster point should be fortified to delay external entry.
- A safe muster point should have access to independent external communication such as portable VHF and satellite communication. A list of key emergency numbers should be also made available at the safe muster point.
- A safe muster point should be located where the crew is not visible to the perpetrators and vulnerable to attack.

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

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

Citadels

If citadels are to be employed, they should be complementary to, rather than a replacement for, all other Ship Protection Measures set out in the guide. The establishing of a citadel may be beyond the capability of the ship's staff alone, and may well require external technical advice and support.

- A citadel is designed and constructed to resist a determined attack and protect the crew.
- The citadel should be safe, secure and well ventilated in line with health and safety regulations.
- The successful use of citadels is predicated on intervention by maritime enforcement agencies.
- Provisions such as food, water, first aid and sanitation should be provided for at least 72 hours. Control of propulsion and steering can offer effective protection during an attack.
- A citadel should have access to independent external communication such as portable VHF and satellite communication. A list of key emergency numbers must be made available in the citadel.
- The use of the citadel must be rehearsed to ensure the Master is able to make the correct and timely decision on whether to retreat into it or not. The ship's SSP should define the conditions for use of the citadel.
- The whole concept of the citadel approach is lost if any crew member is left outside before it is secured.
- The use of a citadel cannot guarantee a law enforcement/military response. The crew may have to decide to discontinue use of a citadel without the assistance of law enforcement/military resources.

Courtesy of ReCAAP Focal Point (India)

Additional protection measures may also include:

- An independent tracking system with independent transmitters
- Motion sensors
- Door sensors

SECTION 8
ROUTINE SHIP SECURITY REPORTING

The Asian region is composed of functioning States that apply the rule of law. Law enforcement agencies and naval forces are operating in the region and in close cooperation with each other. The IMO advocates reporting incidents to the nearest coastal States as they have the jurisdiction and responsibility to enforce the law and prevent maritime crimes.

The VCR scheme has been established by the IFC in Singapore for the purpose of routine ships security reporting and enhancing maritime security for all merchant ships operating in the IFC's VCR area.

Merchant ships operating in the VCR area are strongly encouraged to participate in this reporting scheme by submitting routine security reports and reporting maritime security incidents or anomalous behaviour to the IFC. Participation in this reporting scheme is totally free and ships sailing under any flag are strongly encouraged to participate. All information provided is treated with strict commercial confidentiality and will be used only by the military and maritime enforcement agencies.

Reporting

- It is strongly recommended that ships participate in the VCR scheme when ships are in the VCR area as per Maritime Security Chart Q6112 and Q6113.
- Maintain regular contact with the CSO and report suspicious activity to the IFC and relevant ReCAAP Focal Point. This will give Masters greater situational awareness.
- Reports provided by ships operating in the VCR area will give regional authorities and agencies greater knowledge of activities in their areas of interest.

IFC provides ships participating in the reporting scheme with maritime security advisories based on their reported position and intended destinations where applicable and appropriate. IFC will evaluate and monitor selected ships and share the information with other maritime enforcement agencies when required. Consistent reporting will allow IFC to pass on valuable information to the relevant maritime enforcement agencies in the event of an incident and aid in their timely response to incidents. Refer to **Annex C** for more details on the VCR scheme.

In the event of an attack, the procedure detailed in Section 9 should be strictly followed.

SECTION 9
SHIPS UNDER ATTACK

A. Approach Stage

Majority of attacks in Asia are conducted from small boats in areas where there may be concentration of small boat activities. Ships' reaction time may be short due to their proximity and difficulties in discerning the small boats' intentions, especially at night. Hence, there is need for vigilant lookouts, both visual and radar.

If ships suspect that an attack is imminent, or if in doubt, the crew should implement the Company's security plan which is recommended to include the following steps:

- Sound an alarm to signal an attack may be imminent or in progress.
- Activate the SSAS which will alert your CSO and flag State.
- Make an announcement in accordance with the Ship's Emergency Plan.
- Activate Ship's emergency communication plan, including making a mayday call on VHF Ch. 16. Send a distress message via the Digital Selective Calling (DSC) system and Inmarsat-C, as applicable.
- Report the attack immediately to the Maritime Rescue Coordination Centre (MRCC), CSO and the IMB. Maintain contact with the authorities of coastal States preferably by telephone for as long as it is safe to do so (Refer to **Annex D** for contact details for MRCC and IMB PRC).
- CSO should alert flag State, ReCAAP Focal Point (See **Annex D**), and IFC (where possible). Muster the crew according to procedures.
- Place the ship's whistle/foghorn/alarm on auto mode to demonstrate to any potential attacker that the crew is aware of the attack and is reacting to it.
- Transmit out a distress alert.
- Ensure that the AIS is switched ON.
- Procedures should be in place to ensure the safety of the crew.
- Confirm that the designated entry point to the accommodation is fully secured.
- Activate water spray.
- Speed should be increased as much as possible to widen the distance between the ship and the perpetrators' boat. Try to steer a straight course to maintain maximum speed. Consider evasive actions if the circumstance warrants it.

- If possible, alter course away from the approaching craft. When sea conditions allow, consider altering course to increase an approaching craft's exposure to wind/waves.
- Confirm that all doors are secured and all crew members are mustered within the safe muster point or citadel. Master to then make the final decision to evacuate the bridge if safe to do so. Take all way off, stop engines and display Not Under Command (NUC) lights.
- Switch on additional lighting during the hours of darkness.
- Report the attack as soon as possible to the nearest coastal State through its MRCC. In addition, report to the CSO (who will inform the flag State and Focal Point); and contact IMB by phone if the situation permits.

B. During an Attack

- Reconfirm all ship's crew are in the safe muster point or citadel as instructed by the Master.
- Ensure the SSAS has been activated.
- If not actioned, report the attack immediately to the MRCC, CSO and the IMB. Maintain contact with the authorities of coastal States preferably by telephone for as long as it is safe to do so (Refer to **Annex D** for contact details for MRCC and IMB PRC).
- As the attackers close in on the ship, Masters should commence small alterations of helm whilst maintaining speed to deter perpetrators' boats from lying alongside the ship in preparation for a boarding attempt. These manoeuvres will create additional wash to impede the operation of the boats.
- Large amounts of helm are not recommended, as these are likely to significantly reduce a ship's speed.
- Check Voyage Data Recorder (VDR) data is being saved.
- All remaining crew members to proceed to the citadel or safe muster point locking all internal doors on route.
- Establish communications from the citadel with MRCC and your company and confirm all crew are accounted for and in the citadel or safe muster point.
- Stay in the citadel until conditions force you to leave or advised by the military.
- If any member of the crew is captured, it should be considered that the pirates have full control of the ship.

C. Incident reporting

The Appendix 2 of the IMO circular MSC.1/Circ. 1334 on '*Guidance to shipowner and ship operator, shipmaster and crews on preventing and suppressing acts of piracy and armed robbery against ships*' depicts the incident reporting and information sharing processes in the Asian region (**Annex B**).

In the event of an actual attack or attempted attack,

a. The Master should alert:

(i) the nearest coastal State through its MRCC
(ii) the CSO
(iii) IMB

The MRCC information is available in the Admiralty List of Radio Signals Maritime Radio Stations, The Mariner's handbook, and Search and Rescue Contacts. Ship master is advised to have the updated information readily available on board. You may refer to the following for more details:

- NP 281 Admiralty List of Radio Signals Maritime Radio Stations Europe, Africa and Asia 2015/2016 Ed
- NP 100 The Mariner's Handbook
- Search and Rescue Contacts (http://sarcontacts.info/)

b. The CSO should alert:

(i) the flag State
(ii) ReCAAP Focal Point (Refer to **Annex D**)

c. Where possible, alert:

(i) IFC

SECTION 10
ACTIONS FOLLOWING ILLEGAL BOARDING

The majority of incidents in Asia involve perpetrators who tend to avoid confrontation with the crew. However, there were incidents in which the perpetrators used violence to subdue the crew. Therefore, it is important that the Master and crew:

- Do not engage in a confrontation with the perpetrators because this may put the crew at the risk of getting hurt or killed.
- Remain calm. Stay positive.
- Follow the perpetrators' orders. All crew's movements should be calm, slow and very deliberate.
- Do not resist when the perpetrators reach the bridge. Compliance with perpetrators is essential once a ship has been taken.
- Crew should keep their hands visible at all times.
- Do not attempt to take photographs.
- If the bridge/engine room is to be evacuated, the main engine should be stopped and all way taken off the ship if possible (and if navigationally safe to do so).
- Keep all CCTV and VDR recording devices running.

Past incidents have shown that perpetrators generally boarded the ship, stole the ship's stores and personal belongings and escaped immediately. There have been kidnapping incidents in Asia, but fortunately the number of such incidents has decreased.

In the event that enforcement agencies take actions on board the ship, all personnel should keep low to the deck and cover their head with both hands, with hands visible. On no account should the crew make movements that could be misinterpreted as being aggressive. It is very important that nothing should be pointed at military personnel and flash photography must not be used.

Masters and CSOs should brief and prepare the ship's crew to cooperate fully during any enforcement action on board.

SECTION 11
PRESERVING EVIDENCE

The period following an attack would be confusing as Companies, Masters and Crew recover from the ordeal. To give the investigating authorities the best chance of apprehending the perpetrators, it is important that evidence is collected and preserved in the correct manner. Companies, Masters and Crew should refer to IMO Guidelines on the Preservation and Collection of Evidence reference A28/Res. 1091 and other industry guidance on this area.

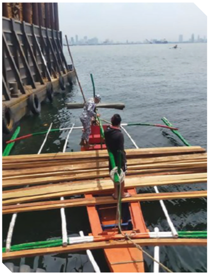
Protection of evidence The Master and crew can protect a crime scene until the nominated law enforcement agency arrives by following these basic principles:

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

Investigation. The quality of the evidence provided and the availability of the crew to testify will significantly help any investigation or prosecution that follows. Following any attack or incident, the investigating authority will be determined by external factors including:

- Flag State.
- Ownership.
- Crew nationality. The lead law enforcement agency will talk to the Master and crew to understand the sequence and circumstances of the event. In a post hostage situation, law enforcement authorities may ask to conduct post-release crew debriefs and to collect evidence for investigations and prosecutions following captivity.

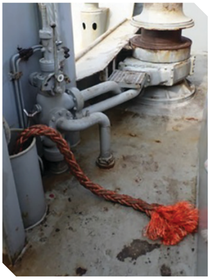
Advice. INTERPOL can provide support to ship operators who have had their ships hijacked. INTERPOL's Maritime Security Sub-Directorate can assist in taking the appropriate steps to preserve the integrity of the evidence left behind at the crime scene. It is recommended that ship operators contact INTERPOL as soon as possible ideally within 3 days of a hijacking of their ship. INTERPOL may be consulted to discuss the recommended practices for the preservation of evidence that could be useful to law enforcement agencies in its investigation. INTERPOL has a Command and Coordination Centre (CCC) that supports its member countries faced with a crisis or requiring urgent operational assistance. The contact details of the CCC is in **Annex D**.



Stolen timber onboard perpetrators' motor banca (Courtesy of ReCAAP Focal Point (Philippines))

Ransack of cabin (Courtesy of ReCAAP Focal Point (Thailand))

Hand-made cigarette bottle by perpetrators (Courtesy of ReCAAP Focal Point (Vietnam))



Part of stolen mooring rope (Courtesy of Swire Pacific Offshore Operations (Pte) Ltd)

SECTION 12
POST-INCIDENT REPORTING

Following an attack, it is vital that a detailed report of the incident be provided to several recipients:

Flag State

Individual flag State will require a detailed report on the incident. Reference should be made to the relevant legislation.

ReCAAP Focal Point, IFC and IMB

It is important that a detailed report of the incident is provided to ReCAAP Focal Points, IFC and IMB. This will enhance knowledge of the activity in the maritime domain and better tailor future warnings or advice these regional reporting centres issue to the maritime community. The report should follow the format contained in **Annex E** (for contact details, see **Annex D**).

Coastal State

It is essential that every incident is reported to the nearest coastal States to assist them in fulfilling their obligations under UNCLOS, to implement law enforcement and to encourage the international community to support infrastructure and capacity building in the region. The Asian region is bounded by functioning governments who understand the maritime domain, operate the Vessel Traffic Information System (VTIS) and have law enforcement and naval assets to deploy for patrols and in response to reports of incidents of piracy and armed robbery.

INTERPOL

INTERPOL maintains an extensive database containing information about pirates and their networks. The collection of information after an attack is vital to ensure that evidence can be gathered in order to support successful prosecutions. Therefore, informing INTERPOL and allowing authorities to collect evidence is of great importance in assisting the prosecuting authorities.

SECTION 13
OTHER CONSIDERATIONS

Companies should actively assist seafarers to overcome the trauma suffered from an attack. The assistance should recognise that those involved may have suffered both physical and mental trauma. The same applies to the families of the seafarers as they also suffer at home. There are a number of international programmes run by Non-Governmental Organizations (NGOs) that can provide advice on the after-care and support of seafarers and their families. Such schemes are run by the International Seafarers Welfare and Assistance Network (ISWAN) and the Mission to Seafarers. Further information can be gained from https://www.seafarerswelfare.org/ and https://www.missiontoseafarers.org.

ANNEX A
DEFINITIONS

1. As defined in Article 101 of the United Nations Convention on the Law of the Sea (UNCLOS):

   "**Piracy**" means any of the following acts:

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

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

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

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

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

2. As defined in the Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery against Ships of the International Maritime Organisation (IMO) Assembly Resolution A.1025(26):

   "**Armed robbery against ships**" means any of the following acts:

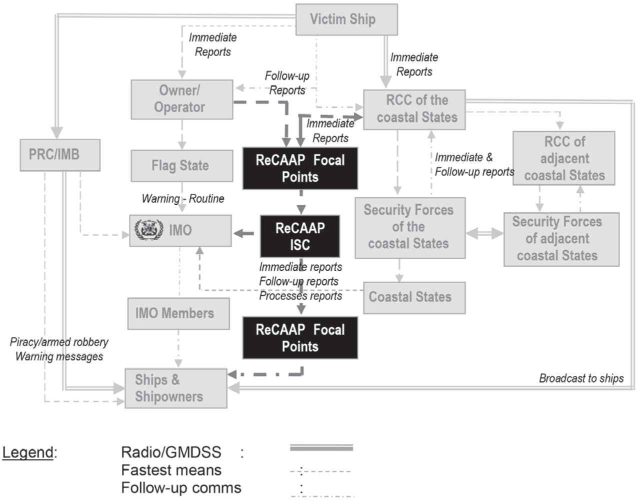
   (a) any illegal act of violence or detention, or any act of depredation, or threat thereof, other than an act of "piracy", committed for private ends and directed against a ship, or against persons or property on board such ship, within a State's internal waters, archipelagic waters and territorial sea;

   (b) any act of inciting or of intentionally facilitating an act described above.

ANNEX B
IMO CIRCULAR (INCIDENTS REPORTING IN ASIA)

The key principle of respecting a coastal State's sovereignty takes precedence over enforcement action in their area of jurisdiction. It also supports the reporting of incidents of piracy and armed robbery against ships to the nearest coastal States as advocated by the IMO Circular MSC.1/ Circ. 1334 on '*Guidance to shipowners and shipoperators, ship master and crews on preventing and suppressing acts of piracy and armed robbery against ships*'. The flow diagram for reporting incidents in Asia found in Appendix 2 of the Circular is shown below.

FLOW DIAGRAM FOR REPORTING INCIDENTS IN ASIA



NOTES:

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

ANNEX C
VOLUNTARY COMMUNITY REPORTING

The Voluntary Community Reporting (VCR) scheme as depicted in MARSEC charts Q6112 and Q6113 has been established by the IFC for the purpose of enhancing maritime security for all merchant ships operating in the IFC Voluntary Community Reporting (VCR) area. The IFC has expanded the VCR area to be consistent with IFC's Area of Interest which has grown with more International Liaison Officers joining the IFC. The new VCR area will be reflected in future updates of the charts Q6112 and Q6113.

Merchant ships operating in the VCR region are encouraged to report maritime security incidents or anomalous behaviour to the IFC. This includes cyber attack incidents and any interference that is observed on RF, GPS, and radars. The Owners/Masters of the ships are encouraged to send regular reports of their position/course/speed and other voyage information as well as report on anomalous activities to the IFC. In return, IFC provides maritime security advisories to the ships based on their reported position and intended destinations. IFC will evaluate and monitor selected ships, and share the information with other maritime enforcement agencies when required. Ships are encouraged to report under the following conditions:

i. On entering the VCR Area using the IFC Initial Report form.
ii. Report ship positional information by either using the "IFC Position Report" at ship's desired intervals or add IFC to their reporting distribution list while reporting positional information to their company.
iii. Observing any suspicious or anomalous behaviour using the Suspicious / Irregular Activity Report.
iv. On exiting the VCR Area using the IFC Final Report form.

Participation in this reporting scheme is encouraged. All information provided is treated with strict commercial confidentiality and will be used within the military and maritime enforcement agencies.

Anomalies are behaviours outside the normal expectations of shipping, commercial trade, or marine practice. They may be indicative of a maritime security threat. These can include, but are not limited to, the following:

- Unusual RVs of ships at sea including transfers of cargo or people
- Darkened ships/not illuminating navigation lights
- Ships anchored in unusual locations
- Ships not flying a flag/displaying a name
- Ships navigating contrary to the ordinary practice of seamen
- Ships outside of normal patterns/sea lanes
- Fishing boat without appropriate equipment
- Overcrowded/unseaworthy/overloaded ships
- Non-ocean going ships in the high seas
- Abandoned ships
- Unwarranted/unsolicited approaches by ships to your own ship or other ships in your vicinity
- Non-military/government ships carrying arms
- Ships carrying boarding equipment
- Suspicious/unusual voice communications
- Shipsunderway/making way without AIS transmission

Send the Initial Report, Daily/Transit Position Report, Final Report and Suspicious / Irregular Activity Report to IFC by email to information_fusion_centre@defence.gov.sg using the relevant report format shown on this chart or telephone +65 6594 5728 or +65 9626 8965.

The IFC's recommended reporting format has been aligned to the United Kingdom Maritime Trade Operations (UKMTO) format, however it is not mandatory to send using the recommended format if ships already have their own reporting format. Ships can just add IFC into their distribution list to simplify the reporting process.

Ships are requested to inform the IFC when they have entered the VCR area.

IFC Initial Report	
01	Ship Name
02	Flag
03	IMO Number
04	Inmarsat Telephone Number
05	Time & Position
06	Course
07	Passage Speed
08	Freeboard
09	Cargo
10	Destination and Estimated Time of Arrival
11	Name and Contact of Company Security Officer
12	Nationality of Master and Crew
13	Armed/Unarmed Security Team Embarked

Ships can also add IFC to their email distribution list when providing positional updates to their companies as per their company timelines.

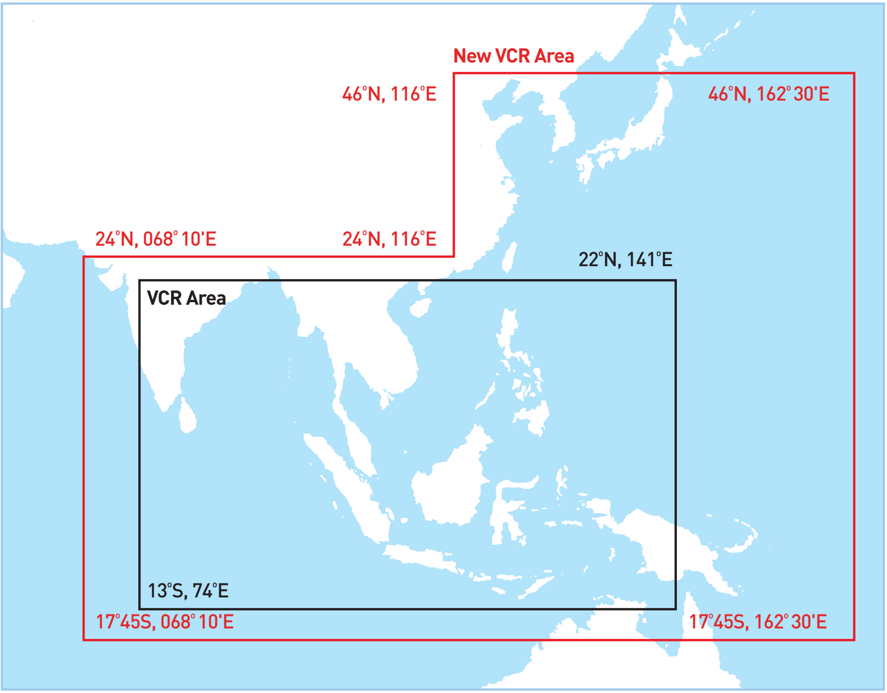
Daily/Transit Position Report	
01	Ship Name
02	Ship's Call Sign and IMO Number
03	Time of Report in UTC
04	Ship's Position
05	Ship's Course and Speed
06	Any other important information (E.g. Change of destination or ETA, number of crew on board, etc)

Ships are requested to inform the IFC via email when they have exited the VCR Area.

IFC Final Report	
01	Ship Name
02	Ship's Call Sign and IMO Number
03	Time of Report in UTC
04	Port or position when leaving the VCR Area

Suspicious / Irregular Activity Report	
01	Ship Name
02	Ship's Call Sign and IMO Number
03	Time of Report in UTC
04	Ship's Position
05	Ship's Course and Speed
06	Sighting of suspicious activity. Time, position, brief description of craft and activity witnessed

IFC VOLUNTARY COMMUNITY REPORTING AREA



ANNEX D
CONTACT DETAILS

Refer to the ReCAAP ISC website (at www.recaap.org) for the updated contact details of the ReCAAP Focal Points and Contact Point.

	Contact Details	
ReCAAP ISC	Phone No	Fax Number
ReCAAP Information Sharing Centre (ISC) Email: info@recaap.org	+65-6376-3091	+ 65-6376-3066

ReCAAP Focal Points / Contact point		
Country & Agency In Charge	Contact Details	
	Phone No	Fax Number
Australia (ReCAAP Focal Point)		
Australian Maritime Border Operations Centre (AMBOC) Maritime Border Command (MBC) E-mail: amboc@border.gov.au	+61-2-6275-6000	+61-2-6275-6275
Bangladesh (ReCAAP Focal Point)		
Department of Shipping E-mail: cns@dos.gov.bd	+88-02-9553584	+88-02-9587301
Brunei (ReCAAP Focal Point)		
National Maritime Coordination Centre Brunei Email: p2mk@jpm.gov.bn	+673-2233751	+673-2233753
Cambodia (ReCAAP Focal Point)		
Merchant Marine Department E-mail: mmd@online.com.kh	+85-5-2386-4110	+85-5-2386-4110

Country & Agency In Charge	Contact Details	
	Phone No	Fax Number
China		
China Maritime Search and Rescue Centre (Beijing) Email: cnmrcc@mot.gov.cn	+86-10-6529-2218 +86-10-6529-2219 +86-10-6529-2221	+86-10-6529-2245
Maritime Rescue Coordination Centre (Hong Kong) Email: hkmrcc@mardep.gov.hk	+85-2-2233-7999 +85-2-2233-7998	+85-2-2541-7714
Denmark		
Danish Maritime Authority (DMA) Email: ReCAAP-FP-DK@dma.dk	+45-9137-6000	+45-9137-6001
Germany		
Federal Police Germany Department for Maritime Security Piracy Prevention Centre (PPC) E-mail: bpol.see.ppz@polizei.bund.de	+49 4561-4071-3333	+49 3020-4561-2198
India		
MRCC (Mumbai) C/o Headquarters Coast Guard Region (West) Mumbai – India E-mail: mrcc-west@indiancoastguard.nic.in mrcc.mumbai@gmail.com	+91-22-2431-6558 +91-22-2438-8065 +91-22-2438-3592	+91-22-2431-6558 +91-22-2438-8065 +91-22-2438-3592
Japan		
Japan Coast Guard (JCG) Ops Centre E-mail: jcg-op@mlit.go.jp	+81-3-3591-9812 +81-3-3591-6361	+81-3-3581-2853

Country & Agency In Charge	Contact Details	
	Phone No	Fax Number
Republic of Korea		
Situation Room (Operation Centre) Ministry of Oceans and Fisheries Email: mof5896@korea.kr	+82-44-200-5895 to 98	+82-44-200-5238
Laos		
International Organisations Department UN Political and Security Affairs Division Ministry of Foreign Affairs E-mail: unpolsec.mfalaos@gmail.com	+856-21-414025	+856-21-414025
Myanmar		
MRCC Ayeyarwaddy Myanmar Navy E-mail: mrcc.yangon@mptmail.com.mm mrcc.myanmar2012@gmail.com	+95-313-1651 +95-979-527-9576 (Mobile)	+95-1-8202-417
Netherlands		
Dutch Coast Guard Maritime Information Centre E-mail: mik-nl@kustwacht.nl	+31-223 658-101	+31-223-658-358
Norway		
Norwegian Maritime Authority Email: security@sdir.no	+47-52-74-5000	+ 47-52-745-001
Philippines		
Philippine Coast Guard Command Center Email: pcgcomcen@coastguard.gov.ph	+632-8-527-3877 (loc 6136/6137) +632-918-803-5327 / +632-917-842-8249 (mobile)	+632-8-527-3877

Country & Agency In Charge	Contact Details	
	Phone No	Fax Number
Singapore		
Maritime and Port Authority of Singapore Port Operations Control Centre (POCC) E-mail: pocc@mpa.gov.sg	+65-6226-5539 +65-6325-2493	+65-6227- 9971 +65-6224-5776
Sri Lanka		
Sri Lanka Navy Operations Room (MRCC-Colombo) Email: nhqdno@yahoo.com nhqdno@navy.lk	+94-11-2445368 +94-11 2212230/31	+94-11-244-1454 +94-11-244-9718
Thailand		
Royal Thai Navy Maritime Information Sharing Centre (MISC) Email: miscdutyofficer@misc.go.th sornchon2558@gmail.com	+66-2475-4532	+66-2475-4577
United Kingdom		
National Maritime Information Centre Operations Centre Email: JMSC-NMICOps@mod.gov.uk	+44 2392 211941	+44 2392 212024 Please indicate "FAO NMIC – A Leg" if send by fax
United States		
USCG Rescue Coordination Center Alameda (RCC Alameda) Email: rccalameda1@uscg.mil	+1-510-437-3701	+1-510-437-3017
Vietnam		
Vietnam Coast Guard Email: vietnamcoastguard@gmail.com	+84-24-3355-4378	+84-24-3355-4363

Information Fusion Centre		
Information Fusion Centre (IFC) Email: Information_fusion_centre@defence.gov.sg	+65-9626-8965 (24/7 Hotline) +65-6594-5728 (office)	+65-6594-5734
Indonesia		
Badan Keamanan Laut Republic Indonesia (BAKAMLA) Email: humas@bakamla.go.id	+62 21-50848130	
Malaysia		
Malaysian Maritime Enforcement Agency (MMEA)		
Kedah/Perlis State	+604-9662750	+604-9660542
Penang State	+604-2626146	+604-2636444 +604-2645052
Perak State	+605-6804116	+605-6833741
Selangor State	+603-31769100	+603-31765100
Johor State	+607-2199440	+607-2199451
Melaka & Negeri Sembilan	+606-3876730 +606-3876811	+606-3876827
Pahang State	+609-5717300	+609-5738476
Terengganu State	+609-6223657	+609-6224163
Kelantan State	+609-7780070 +6014-5384106	+609-7780075
Sabah State	+608-8387774	+608-8270105
Sarawak State	+608-2432544 +608-2432006 +608-2432016 +608-2423019	+608-2432502 +608-2432554

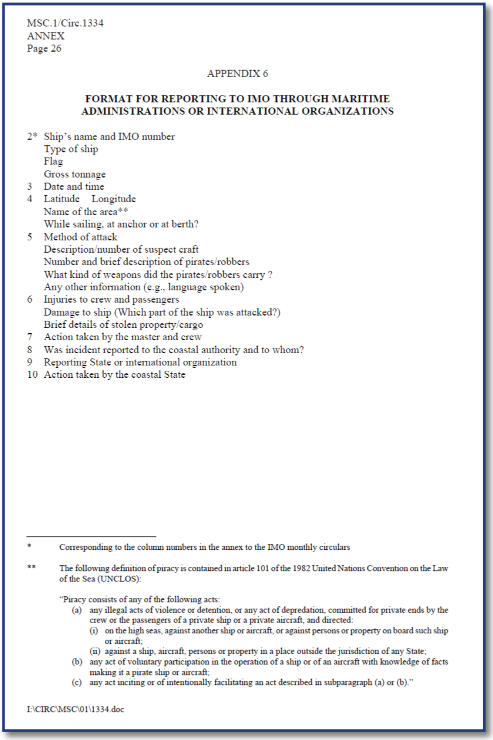
INTERPOL		
Command and Coordination Centre (CCC) [Operates in all four of INTERPOL's official languages (English, French, Spanish and Arabic)] Email: os-ccc@interpol.int	+33 474 44 76 76 (24/7 Hotline)	
International Maritime Bureau (IMB)		
IMB Piracy Reporting Centre 24 Hrs Anti-Piracy Helpline General Email: imbkl@icc-ccs.org Piracy Email: Piracy@icc-ccs.org	+603 2031 0014	+603 2078 5768

🟦 ReCAAP Focal Points 🟧 Other Agencies

Last Updated on 31 Dec 2021

ANNEX E
PIRACY ATTACK REPORT

Following any attack or sighting of suspicious activity, it is vital that a detailed report of the incident is sent to ReCAAP Focal Points, IFC and IMB via e-mail or fax. The appropriate and relevant information from an incident will be used to support INTERPOL and regional law enforcement investigations. The format of the piracy attack report is in accordance with Appendix 6 of the IMO Circular MSC.1/ Circ 1334 on '*Guidance to shipowners and ship operators, shipmaster and crews on preventing and suppressing acts of piracy and armed robbery against ships*'.



MSC.1/Circ.1334
ANNEX
Page 26

APPENDIX 6

FORMAT FOR REPORTING TO IMO THROUGH MARITIME ADMINISTRATIONS OR INTERNATIONAL ORGANIZATIONS

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

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

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

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

I:\CIRC\MSC\01\1334.doc

ANNEX F
ReCAAP ISC AND WORKING GROUP

ReCAAP ISC

The Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) is the first regional government-to-government agreement to promote and enhance cooperation against piracy and armed robbery in Asia. It was finalized on 11 November 2004 and entered into force on 4 September 2006. To date, 21 States have become Contracting Parties to ReCAAP.

The 21 Contracting Parties to ReCAAP are Australia, the People's Republic of Bangladesh, Brunei Darussalam, the Kingdom of Cambodia, the People's Republic of China, the Kingdom of Denmark, the Federal Republic of Germany, the Republic of India, Japan, the Republic of Korea, the Lao People's Democratic Republic, the Republic of the Union of Myanmar, the Kingdom of the Netherlands, the Kingdom of Norway, the Republic of the Philippines, the Republic of Singapore, the Democratic Socialist Republic of Sri Lanka, the Kingdom of Thailand, the United Kingdom, the United States of America and the Socialist Republic of Viet Nam.

The ReCAAP Information Sharing Centre (ReCAAP ISC) was established under the Agreement, and was officially launched in Singapore on 29 November 2006. The roles of the ReCAAP ISC are to:

- serve as a platform for information exchange with the ReCAAP Focal Points via the Information Network System (IFN); facilitate communications and information exchange among participating governments to improve incident response by member countries; analyse and provide accurate statistics of the piracy and armed robbery incidents to foster better understanding of the situation in Asia;
- facilitate capacity building efforts that help improve the capability of member countries in combating piracy and armed robbery in the region; and
- cooperate with organizations and like-minded parties on joint exercises, information sharing, capacity building programme, or other forms of cooperation, as appropriate, and agreed upon among the Contracting Parties.

The ReCAAP ISC facilitates exchange of information among the ReCAAP Focal Points through a secure web-based IFN. Through this network, the ReCAAP Focal Points are linked to each other as well as the ReCAAP ISC on a 24/7 basis, and are able to facilitate appropriate responses to incident. The agency receiving the incident report will manage the incident in accordance with its national policies and response procedures, and provide assistance to the victim ship where possible. The agency will in turn, inform their ReCAAP Focal Point which will submit an incident report to the ReCAAP ISC and its neighbouring Focal Points. The list of ReCAAP Focal Points and Contact Point are tabulated below. For more information about the ReCAAP and ReCAAP ISC, please visit http://www.recaap.org.

ReCAAP FOCAL POINTS / CONTACT POINT	
ReCAAP Focal Point (Australia)	Maritime Border Command (MBC)
ReCAAP Focal Point (Bangladesh)	Department of Shipping
ReCAAP Focal Point (Brunei)	National Maritime Coordination Centre
ReCAAP Focal Point (Cambodia)	Merchant Marine Department
ReCAAP Focal Point (China)	China Maritime Search and Rescue Centre (Beijing)
ReCAAP Contact Point (Hong Kong)	Maritime Rescue Coordination Centre (Hong Kong)
ReCAAP Focal Point (Denmark)	Danish Maritime Authority
ReCAAP Focal Point (Germany)	Federal Police Germany
ReCAAP Focal Point (India)	Indian Coast Guard
ReCAAP Focal Point (Japan)	Japan Coast Guard
ReCAAP Focal Point (Republic of Korea)	Ministry of Oceans and Fisheries
ReCAAP Focal Point (Laos)	Ministry of Public Security
ReCAAP Focal Point (Myanmar)	Myanmar Navy
ReCAAP Focal Point (Netherlands)	Dutch Coast Guard
ReCAAP Focal Point (Norway)	Norwegian Maritime Authority
ReCAAP Focal Point (Philippines)	Philippines Coast Guard
ReCAAP Focal Point (Singapore)	Maritime and Port Authority of Singapore
ReCAAP Focal Point (Sri Lanka)	Sri Lanka Navy
ReCAAP Focal Point (Thailand)	Royal Thai Navy
ReCAAP Focal Point (United Kingdom)	National Maritime Information Centre
ReCAAP Focal Point (United States)	US Coast Guard
ReCAAP Focal Point (Vietnam)	Vietnam Coast Guard

IFC

The Information Fusion Centre or IFC is a 24/7 regional Maritime Security (MARSEC) information-sharing centre, hosted by in the Republic of Singapore Navy. It was inaugurated on 27 Apr 2009 and aims to facilitate information-sharing and collaboration between partners to enhance maritime security. Through the speedy sharing of information, IFC facilitates timely responses with its partner countries on maritime incidents. IFC also aims to achieve early warning of maritime security threats by building a common maritime situation picture and acting as a maritime information hub for the region.

The IFC is manned by an integrated team of International Liaison Officers (ILO) from various navies/coastguards, and RSN personnel. We have wide and extensive linkages with more than 100 linkages in 42 countries. The ILOs serve as the conduit to their respective countries' various agencies' operation centres in facilitating the seamless sharing of information between their parent agencies and the IFC. The IFC works with the shipping community to enhance maritime security through regular activities such as the Shared Awareness Meeting (SAM) and Tiger Team Visits (TTV) to companies.

IFC shares shipping advisories to its shipping partners through its reports such as weekly reports and monthly maps. The IFC also conducts capacity-building activities on international information-sharing exercises and MARSEC workshops such as the biennial Maritime Information Sharing Exercise (MARISX) and the annual Regional Maritime Security Practitioner Course (RMPC). The IFC also hosts maritime information sharing portals such as the ASEAN Information Sharing Portal and the IFC Real-time Information-sharing System (IRIS), which facilitates information sharing among ASEAN navies and Western Pacific Naval Symposium members.
https://www.ifc.org.sg

ASA

The Asian Shipowners' Association (ASA), formally founded as the Asian Shipowners' Forum (ASF) in 1992, is a voluntary organisation of the shipowner associations of Australia, China, Chinese Taipei, Hong Kong, Japan, Korea and the Federation of ASEAN countries (FASA). The ASA shipowners and managers are estimated to control and operate around 50 % of the world's cargo carrying fleet.

The objectives of ASA are to act as a channel to convey Asian Shipowners' voices to the international shipping community as well as to enhance and strengthen the ASA's stature. At the same time, it is also a platform for all ASA members to liaise with one another and to help promote cooperation, amity and friendship amongst its members. Between annual ASA meetings, the ongoing work is carried out by five Standing Committees: Seafarers Committee, Ship Insurance and Liability Committee, Safe Navigation and Environment Committee, Shipping Policy Committee, and Ship Recycling Committee.

FASA

The Federation of ASEAN Shipowners' Associations (FASA), a voluntary trade organisation, comprises the national shipowners' associations from eight ASEAN countries, namely Brunei, Indonesia, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam. The members are strongly motivated by a common desire for closer co-operation in order to increase the role of ASEAN shipping in the carriage of the region's cargoes as well as contribute to the development of intra-ASEAN trade. They also recognise the important need to adopt a common stand on regional and international shipping matters and the development of international trade.

FASA was approved as an ASEAN Non-Governmental Organisation at the 5th Meeting of the 14th ASEAN Standing Committee which was held in Manila on 21 May 1981.

INTERTANKO

International Association of Independent Tanker Owners (INTERTANKO) has been the voice of independent tanker owners since 1970, ensuring that the oil that keeps the world turning is shipped safely, responsibly and competitively.

INTERTANKO is a forum where the industry meets, policies are discussed and statements are created. It is a valuable source of first-hand information, opinions and guidance.

INTERTANKO contributes authoritatively and proactively at international, national, regional and local levels on behalf of the tanker community.

INTERTANKO stands for safe transport, cleaner seas and free competition.

OCIMF

OCIMF focusses on promoting best practice in the design, construction and operation of tankers, barges and offshore vessels and their interfaces with terminals inshore, onshore and offshore. It does so by providing an independent forum for bringing together its members and external stakeholders to leverage their expertise in the creation of publications and programmes that enhance the safety and environmental performance of the marine industry.

SSA

The Singapore Shipping Association (SSA) represents a wide spectrum of shipping companies and other businesses allied to the shipping industry. It is a national trade association formed in 1985 to serve and promote the interests of its members and to enhance the competitiveness of Singapore as an International Maritime Centre.

To achieve its objectives, the SSA plays an active role in promoting the interests of shipping in Singapore and internationally, and co-operates with other regional and international shipping organisations to protect the marine environment and promote freedom and safety at sea.

Currently SSA represents some 470 member companies; comprising shipowners and operators, ship managers, ship agents and other ancillary companies such as shipbrokers, classification societies, marine insurers, bunker suppliers, maritime lawyers, and shipping bankers amongst others.

RSIS

The S. Rajaratnam School of International Studies (RSIS) is a global think tank and professional graduate school of international affairs at the Nanyang Technological University, Singapore. An autonomous school, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. With the core functions of research, graduate education, and networking, it produces research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-traditional Security, Cybersecurity, Maritime Security and Terrorism Studies.

For more details, please visit www.rsis.edu.sg. Join us at our social media channels at www.rsis.edu.sg/rsis-social-media-channels or scan the QR code.

LIST OF ABBREVIATIONS AND ACRONYMS

AIS	Automatic Identification System
ASG	Abu Sayyaf Group
CCC	Command and Coordination Centre
CCTV	Closed-circuit Television
CSO	Company Security Officer
DSC	Digital Selective Calling
F(P)SO	Floating (Production) Storage & Offloading
IFN	Information Network System
ISPS	International Ship and Port Facility Security
MARSEC	Maritime Security
MRCC	Maritime Rescue Coordination Centre
NAVAREA	Navigational Area
NGO	Non-Governmental Organization
NUC	Not Under Command
PCASP	Privately Contracted Armed Security Personnel
PMSCs	Private Maritime Security Contractors
RCC	Rescue Coordination Centre
SOMS	Straits of Malacca and Singapore
SS	Singapore Strait
SSA	Ship Security Assessment
SSO	Ship Security Officer
SSAS	Ship Security Alert System
SSP	Ship Security Plan
STS	Ship to Ship
TaB Guide	Tugs and Barges Guide
TSS	Traffic Separation Scheme
UNCLOS	1982 UN Convention on the Law of the Sea
VCR	Voluntary Community Reporting
VDR	Voyage Data Recorder
VHF	Very High Frequency
VHP	Vessel Hardening Plan
VTIS	Vessel Traffic Information System

ReCAAP

Information Sharing Centre

Regional Cooperation Agreement on Combating Piracy and Armed Robberyagainst Ships in Asia
21 Media Circle, #05-04, Singapore 138562
T +65 6376 3091 | F +65 6376 3066 | E info@recaap.org | W www.recaap.org