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

Working Group:

ReCAAP Information Sharing Centre

IFC INFORMATION FUSION CENTRE

RSiS Nanyang Technological University | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

ASIAN SHIPOWNERS FORUM

FEDERATION OF ASIAN SHIPOWNERS' ASSOCIATIONS

INTERTANKO

OCIMF

SSA SINGAPORE SHIPPING ASSOCIATION

CONTENTS

SECTION 1
INTRODUCTION

Piracy and armed robbery in the Asian region has been evolving over time. The definitions of 'piracy' (in accordance with UNCLOS) and 'armed robbery against ships' (in accordance with IMO) can be found in **Annex A**. The Asian region in this guide refers to the area as marked on Marsec Charts Q6112 and Q6113 (**Annex B**).

It should be noted that piracy and armed robbery in Asia differs significantly from that of Somalia-based piracy. While Somalian-based pirates generally attacked ships in order to hijack them and then hold the crew for ransom, the type of criminal activity occurring in Asian waters generally revolves around theft of personal property and hijacking of ships for the purpose of cargo theft. Although the common modus operandi in the region has not changed significantly in the last decade, there were some trends in recent years which have attracted attention. The *Tug Boats and Barges (TaB) Guide Against Piracy and Sea Robbery* launched in January 2013 was a response to the increase in number of incidents involving tug boats and barges between 2008 and 2012. A spike in the number of incidents involving oil cargo theft from 2014-2015 prompted the release of the *Guide for Tankers Operating in Asia against Piracy and Armed Robbery Involving Oil Cargo Theft* in November 2015.

Beyond the more specific trends involving particular types of ships, it is notable that the last four years (2012-2015) has witnessed a general increase in the number of boardings involving all types of ship while underway and at certain ports and anchorages in Asia. Refer to Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia Information Sharing Centre (ReCAAP ISC)'s website (www.recaap.org) for updates on incidents and trends.

With attacks becoming more widespread and in some cases violent, the maritime community has requested a comprehensive guide which covers all types of ships operating in Asian waters. This guide encompasses the *TaB Guide Against Piracy and Sea Robbery* and *Guide for Tankers Operating in Asia against Piracy and Sea Robbery Involving Oil Cargo Theft;* and will take into consideration the occurrence of incidents involving all types of ship while underway and at ports and anchorages in Asian waters.

SECTION 2
AIM

The purpose of this guide is to assist those responsible for the operation of ships trading in Asia including companies, owners, masters, agents and seafarers in avoiding attacks, deterring attacks and delaying attacks, actions when attacked and evidence preservation.

This guide complements information provided by the relevant resolutions adopted by the United Nations General Assembly and the relevant resolutions and recommendations adopted by the International Maritime Organization (IMO) as in updated MSC Circular 1333/1334 (refer to **Annex C**) and should be read with reference to updated assessments of activity produced by the ReCAAP ISC, the Information Fusion Centre (IFC) and incidents reported by the International Maritime Bureau (IMB).

GEOGRAPHICAL LOCATION

Piracy and armed robbery against ships in Asia varies in approach, so it is difficult to predict the area where a ship might fall victim to piracy or armed robbery. The IFC Voluntary Reporting Area (VRA) is a clearly defined voluntary reporting area, so ship operators and ships transiting, trading or operating in Asia can join a trusted reporting scheme. The IFC encourages ships in the VRA to report to IFC using the reporting format described in Marsec Charts Q6112 and Q6113 when entering the VRA. Please refer to **Annex B**.

Acts of piracy and armed robbery have occurred in the Straits of Malacca and Singapore (SOMS), the southern portion of the South China Sea, within the Indonesia archipelago and at certain ports and anchorages in Asia. For incidents involving tankers for theft of oil cargo, the majority of these occurred within the southern portion of the South China Sea.

In order to determine areas of concern, refer to ReCAAP ISC website for quarterly updates on the latest situation.

Ships should be alert when operating in areas of concern, particularly when they slow down, stop or anchor in areas where attacks are known to occur.

Figure 1: Example of situation map (ReCAAP ISC)

MODUS OPERANDI

A. UNDERWAY
Currently, pirates and armed robbers in Asia are operating for the purposes of theft. Primarily they board ships in order to steal stores and engine spares as well as personal possessions of seafarers. This type of attack affects all ships, big and small, in the region. Hijacking of ships for the purposes of cargo theft has been limited to small parcel tankers carrying refined products which can be sold on various black markets. Attacks, both outside and inside territorial waters, appear to be the result of intelligence-led planning by the pirates, with particular products such as gas oil or gasoline being targeted in well co-ordinated and executed operations. At present, kidnapping of seafarers has not been a major feature of piracy or armed robbery activity in this region. Therefore, criminal activity within Asia can be split broadly into the following categories:

Armed Robbery – In general this is opportunistic, sometimes violent, and occurs where ships are in coastal waters. Ships are particularly vulnerable when at anchor or when the bridge team are involved in navigating through congested waters and island groups. Theft whilst underway occurs in the SOMS, particularly those in the eastern approaches in the Singapore Strait and the South China Sea. The perpetrator's primary aim is to board and leave the ship without being seen and sometimes turn violent when sighted or confronted.

Hijacking – The primary intent is the theft of oil cargo and it is noted that, regionally, these attacks are often referred to as siphoning incidents. Attacks have normally occurred during hours of darkness. They occur primarily in the southern region of the South China Sea; however, several attacks have occurred in the Malacca Strait. These attacks to date have been restricted to small tankers especially those with low freeboard. However, larger tankers should also take the appropriate precautionary measures. There is strong suspicion that the ships are targeted for the specific grade of cargo and indicates that the pirates possess sophisticated intelligence gathering capabilities. Ships can be hijacked for several hours/days and cargo is transferred to a smaller ship which comes alongside. There have been cases where the old identities of the ships were disguised and the seafarers cast adrift in lifeboats, setting them ashore in remote areas. Recent cargo thefts have demonstrated that pirates have knowledge of ship operations allowing them to disable communications, navigate and operate the cargo system. Additionally, there have been a number of incidents where tugs and smaller ships have been taken for resale.

Methodology – Unlike pirates in the Gulf of Aden and West Africa whom are known to use high speed skiffs and long ladders in boarding ships, the perpetrators in Asia often adopt the profile of fishing boats to avoid being noticed and use a variety of tools including poles, hooks and lines to board ships. Additionally, due to the distances involved, the use of motherships has not become widespread.

Simulation of boarding using knotted rope and grapnel hook by arrested sea robbers.
(Courtesy of The Indonesian Navy)

Simulation of how the loot is transferred.
(Courtesy of The Indonesian Navy)

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

In certain ports and anchorages, the risk of armed robbery is particularly high when the ship is at anchor or is drifting off a port for example close to pilot station or conducting STS. Armed robbers often adopt the profile of fishing boats and use local traffic to disguise their approach to those on the bridge of the targeted ship. Particular attention should be paid to any small boats attempting to pass close to your ship. The robbers prefer darkness to make their attack.

STS Operations

The following precautions should be taken during STS operations:

- Vary the location of STS (if operations permit) to avoid setting 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 will have 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.
- 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 a STS operation, other protection measures should be considered to protect the ship from attack in these cases.
- During STS operations or when adrift, equipment such as fenders, anchor chains and hawse pipes can provide a vulnerable point of access for attackers, and entry should be physically blocked.

SECTION 5
RISK ASSESSMENT

For the purpose of identifying suitable measures of prevention, mitigation and recovery in case of piracy or armed robbery, a ship and voyage-specific risk assessment should be carried out prior to entering the sea areas described in Section 3 above to assess the likelihood and consequences of piracy and armed robbery attacks to the ship, based on the latest available information.

Operating in the VRA requires thorough advanced planning, using all available information. The maritime environment is dynamic, the risks and threats will not remain constant for subsequent visits. It is essential that Masters, SSOs and Company Security Officers (CSOs) carry out a detailed Risk Assessment for each voyage to the region and for each activity within the region.

A Risk Assessment is a logical examination of the current situation to identify the risks and threats likely to be encountered. It should examine the effectiveness of security measures already in place and identify additional self-protection measures available. Risk Assessment is a tool to support sound decision making.

The output of this Risk Assessment should identify measures for prevention, mitigation and recovery, combining statutory regulations with supplementary measures to combat piracy and armed robbery. It is important that the Risk Assessment is ship and voyage specific, and not generic. Unlike the Ship Security Assessment (SSA) described in the International Ship and Port Facility Security (ISPS) Code, the Risk Assessment should include, but may not be limited to, the following:

- Crew safety (measures to prevent illegal boarding and external access to the accommodation, whilst ensuring that crew members will not be trapped inside and should be able to escape in the event of another type of emergency, for example fire)
- The specific threat on who are the pirates/armed robbers, what do they want to achieve, how do they attack, how do they board, which weapons do they use etc.

- Background factors shaping the situation (visibility, sea-state, 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 withstand the threat (freeboard, speed, general arrangement etc.)
- Ship's procedures (drills, watch rotation, routine maintenance and activity 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 company, charterer and insurance policies should also be taken into consideration.

In addition to the information found in this document, supplementary information about the characteristics of the threat and regional background factors may be sought from the ReCAAP ISC, IFC, regional reporting centres, shipping association websites, IMB, commercial intelligence providers or local sources e.g. ship's agents.

Ship operators, Masters and CSOs should evaluate and review the effectiveness of the controls already in place to prevent illegal boarding and hijacking of a ship. The evaluation of the effectiveness of the controls already in place and those being implemented as mitigating measures following a voyage specific risk assessment can be greatly assisted by the development of a ship specific hardening plan.

A ship specific hardening plan details the hardening measures being implemented on board the ship including a list of all access routes to the accommodation block and engine room detailing their securing arrangements and status. This plan should be developed by the ship's Master and CSO following an on board security review.

Protection measures discussed in this guidance are generic and designed to promote thought for different ships and circumstances. To maximize effectiveness, a range of tailored measures, most appropriate to the ship and situation in question should be identified and implemented. In order to accurately conduct a risk assessment, the existing self-protection measures (controls) employed must be identified and evaluated. In order to gauge the effectiveness of each measure employed it must be compared with the specific threat it is designed to counter.

Ship protection measures fall into two distinct categories:
• Protection measures installed or provided by the company as part of the Ship Security Plan (SSP).
• Additional measures that may be adopted when the risk of attack increases.

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 pirate modus operandi. Detailed guidance on preparing risk assessments can be found from a variety of sources including the ISPS code.
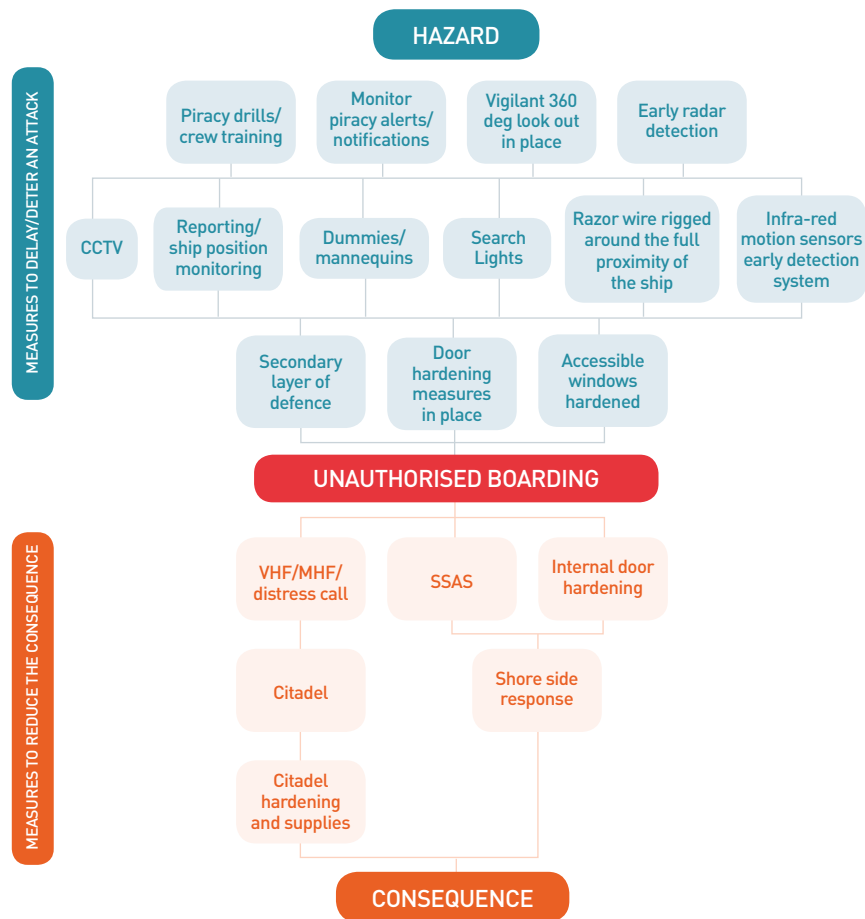

Figure 2: Example of the steps that could be taken following risk assessment

Acceptability
Individual companies will set criteria for what is tolerable risk, and the SSP should mitigate that risk to be as low as practicable. When conducting the risk assessment, it is recommended that risk factors such as freeboard, area, type of ship and speed be taken into consideration.

Record the Assessment
Records of risk assessments should be maintained both by the CSO and on board the ship. These should be reviewed and updated on a regular basis to capture lessons learnt and to highlight gaps. This will generate improvements and provide examples of best practice. Using this experience to educate staff and enhance training aids preparation and readiness. As more people read and understand the risk assessment the greater the level of preparedness becomes and the likelihood of spotting omissions and suggesting improvements increases. The mitigations 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, the onset of calm weather conditions or threat detection; additional control measures need to be predefined and quickly applied to maintain or reduce the risk to an acceptable level.

Considerations for the Master of a Ship:

Before the voyage
Crew Safety
- Ensure that crew members will not be trapped inside the ship, during an attack or during an emergency by the implementation of the hardening measures. All life-saving and fire-fighting appliances must be available for immediate use and emergency escapes must be accessible by the crew.
- Ensure the location of a Safe Muster Point and Citadel, if used, is identified and known to all crew members.
- Attackers may fire weapons at the bridge to force the ship to stop if underway and/or to gain access to the bridge once aboard and to force crew compliance. Consider providing protection around areas of the bridge where bridge team may be required to remain during an attack.

Freeboard
- If a ship is attacked, attackers will often try to board the ship at the stern or the lowest point above the waterline, making it easier for them to climb on board. Additional protective measures should be considered (see section 8).

During the voyage
Speed
- Ships are most vulnerable when stopped in the water, drifting, at anchor or carrying out STS transfer, Single Buoy Mooring (SBM) operations or slowing down for pilot transfer.
- Increase speed to make it difficult for an attacker to board.
- Get underway and/or increase to a maximum safe speed as quickly as possible when a suspicious ship is identified. This will open the distance from any possible attack and make the ship more difficult to board.

Location and Time at Anchor
- Keep time at anchor to a minimum when in area of risk.
- Avoid setting patterns.
- The location of the chosen anchorage position is an important factor in mitigating risks against attacks on the ship.

Sea State
- Ships commonly used by the perpetrators in attacks are usually limited to fair and moderate sea states. It is likely to be more difficult to operate small craft and board an identified ship in sea state three and above.

Reporting
- It is strongly recommended that ships participate in the Voluntary Community Reporting (VCR) scheme when in VRA as per Marsec Charts 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 VRA will give regional authorities and agencies greater knowledge of activities in their areas of interest.

COMPANY PLANNING

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

- **Jointly conduct 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 association websites, commercial intelligence providers or local sources may also be useful in voyage planning.
- **Review the SSA and SSP.** Review the SSA and implementation of the SSP, as required by the ISPS Code.
- **Put SSP in place.** The CSO is encouraged to ensure that a SSP is in place for a passage through the area of concern, and that this is exercised, briefed and discussed with the Master and the SSO.
- **Monitor piracy related websites on specific threats.** Ensure that ships are aware of any specific threats that have been promulgated.
- **Offer guidance to Master with regard to the recommended route.** Offer the ship's Master guidance with regard to the recommended routing through the area of concern and details of the piracy 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 booklet – see Section 8. It has been proven that the use of Ship Protection Measures significantly increases the prospects of a ship resisting an attack.
- **Tracking.** Owners should consider the placement of hidden position transmitting devices as one of the first actions of hijackers is to disable all visible communication and tracking devices and aerials.
- **Conduct crew training.** Conduct crew training sessions (including Citadel drills where utilised) prior to transits with ship protection measures in place.
- **Obtain contact details.** Ensure that contact details of nearest coastal states are readily available and easily accessible. Refer to **Annex D**.
- **Participate in the VCR scheme.** It is strongly recommended that ship operators register with IFC before entering the VRA. Refer to Section 7.

The following important advice should be noted:

- Communications with external parties should be kept to a minimum, with close attention paid to organising rendezvous points and waiting positions. For e-mail correspondence to Agents, Charterers, Chandlers etc. it is strongly recommended that address lists are controlled and that information within the e-mail is concise, containing the minimum that is legally required in order to fulfil requirements or contractual obligations.
- Know your agents and avoid or minimize requirements where possible. Unnecessary interaction with other parties creates opportunities for information regarding the ship's position to be compromised.
- If the ship trades regularly in the region it is recommended to 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 coastal States in the region, and authorities are known to enforce these regulations vigorously.

Unarmed PMSCs are a matter for individual ship operators following their own voyage risk assessment. Consideration should be given to the relevant laws of both Flag States and coastal/Port States in the region. Companies are advised to check with the regional State agencies on PMSC so as not to violate any regional/customary laws/regulations.

MASTER'S PLANNING
··

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

- **Conduct 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 according to the following:
  o Where possible, drifting, waiting and slow steaming should be avoided.
  o Where practicable, a prolonged stay at anchorage is to be avoided. Anchoring within designated anchorage area is strongly encouraged as it deters unauthorised boarding.
  o Minimize use of VHF and use e-mail or secure satellite telephone instead. Where possible only answer known or legitimate callers on the VHF, bearing in mind that imposters are possible.
  o The greatest risks of piracy and armed robbery are during hours of darkness and needs to be factored into all planning. Where possible, operations should start and end during daylight hours.
  o Constant radio watch.
  o Latest NAVAREA warnings and Alerts.
  o Heightened state of readiness 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:
  o Testing the ship's Protection Measures, including testing of the security of all access points.
  o The SSP should be thoroughly reviewed (see Section 6).
  o Lock down conditions, including crew safety considerations.
  o Passage plan should incorporate security considerations.
  o Guidance to bridge team on vigilance stated in night orders.

- **Prepare and Test of Emergency Communication Plan.** Masters are advised to prepare an Emergency Communication Plan, to include all essential emergency contact numbers and prepared messages, which should be ready at hand or permanently displayed near all external communications stations including Safe Muster Point or Citadel (see list of Contacts at **Annex D**). Communication devices and Ship Security Alert System (SSAS) should be tested.
- **Define the ship's Automatic Identification System (AIS) policy.** It is recommended that in an area of concern AIS status be restricted to ship's identity, position, course, speed, navigational status and safety-related information.

Upon entering an area of concern:
- **Reduce maintenance and engineering work to minimum:**
  o Ensure all access points are limited and controlled.
  o All essential equipment is immediately available – appropriate consideration on risk should be given when considering maintenance on essential equipment.

SHIP PROTECTION MEASURES

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

The guidance is based on experience and may require amendment over time if the perpetrators change their modus operandi.

The Ship Protection Measures described 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
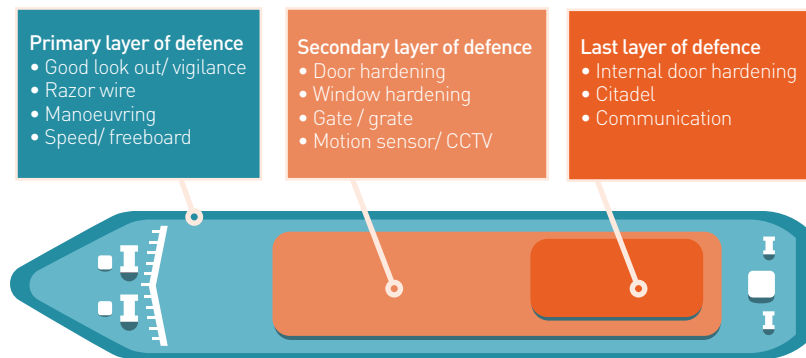- Citadel
- Communication

Figure 3: Example of layered protection

Owners may wish to consider making further alterations to the ship beyond the scope of this booklet, and/or provide additional equipment and/or manpower as a means of further reducing the risk of attack. If perpetrators are unable to board a ship they cannot hijack it.

Watchkeeping and Enhanced Vigilance

- Prior to entering an area of concern, it is recommended that preparations as directed by the risk assessment are made:
  - o Consider a shorter rotation of the Watch period in order to maximise alertness of the lookouts, and ensuring that lookouts are fully briefed and trained.

  - o Ensure that there are sufficient binoculars for the enhanced Bridge Team, preferably anti-glare type.
  - o Consider use of night vision optics.
  - o Maintain a careful radar watch.
  - o Watch for the approaches of small boat from the stern.
  - o Consider enhancing technology where possible, such as monitoring of CCTV.
  - o 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 from the stern.

Enhanced Bridge Protection

- The bridge is usually the focus for any attack. If they are able to board the ship, the perpetrators usually try to go to the bridge to enable them to take control. The following protection enhancements should be considered:
  - o 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.
  - o Fabricated metal (steel/aluminium), hardening for the side and rear bridge windows (for example, consider metal grills or window bars) and the bridge wing door windows, which may be permanently installed or rapidly secured in place in the event of an attack.

Control of Access to Bridge, Accommodation and Machinery Spaces

- It is very important to control the access routes to deter or delay perpetrators who managed to board a ship and are trying to enter accommodation or machinery spaces. It is very important to recognise that if the perpetrators managed to gain access to the upper deck of a ship, they will 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 prior to entry into the area of concern to deny perpetrators' access to the accommodation and the bridge. However escape routes must be easily accessible to seafarers in event of an emergency.

  o All doors and hatches providing access to the bridge, accommodation and machinery spaces should be properly secured to prevent them being opened by perpetrators.

  o Careful consideration should be given to the means of securing doors and hatches in order to afford the ship maximum protection possible.

  o Consideration to installing gates/grates on external stairways.

  o 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 seafarer 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.

  o It is recommended that once doors and hatches are secured, a designated and limited number are used for routine access when required, with their use being strictly controlled.

  o 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 with wire strops may enhance hatch security.

  o 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.

o 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.

o Prior to entering the area of concern, procedures for controlling access to accommodation, machinery spaces and store rooms should be set out and practised.
o Ensure that tools on deck are properly stored away and secured.

Physical Barriers

Perpetrators typically use long lightweight hooked ladders, grappling hooks with rope attached and long hooked poles with a climbing rope attached to board ships 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 hands reduces the risk of injury. It is recommended that razor wire is provided in shorter sections (e.g. 10 metre section) as it is significantly easier and safer to use than larger sections which can be heavier and unwieldy.

• A robust razor wire barrier is particularly effective if it is:
   o 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.
   o 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.
   o When rigging razor wire, care must be taken not to overstretch the wire in order to reduce the amount needed as it becomes ineffective.
• It is recommend that when rigging razor wire, a steel cable is run through the centre in order to offer additional strength and reduce the ability of the hostile attacker being able to pull it down. The added advantage of having the steel cable is for ease of rigging/removal particularly for ships operating on short voyages.
• Although preferably razor wire should be rigged around the full proximity of the ship with a minimum of two layers, this may not be ideal for ships with a low freeboard. To that end, an alternate solution would be to consider using razor wire in front of accommodation in at least 3 layers in order to delay or deter a hostile attacker. If this method is being adopted, due consideration should be given to the security of deck stores and the equipments forward of the barrier.
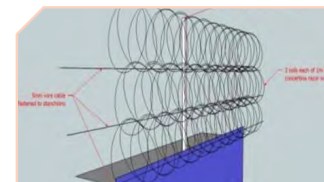
Water Spray and Foam Monitors

The use of water can make it difficult for a suspicious boat to remain alongside and makes it significantly more difficult for a perpetrator to climb on board.

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 it will also save time on hardening 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 ships must be aware this will help protect the accommodation. If this method is being adopted, due consideration should be given to the security of deck stores and the equipment forward of the barrier.

Alarms

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

Sounding the ship's alarms/whistle serves to inform the ship's crew that an attack has commenced and, importantly, demonstrate to any potential attacker that the ship is aware of the attack and is reacting to it. If approached, continuous sounding of the ship's foghorn/whistle distracts the perpetrators and as above lets them know that they have been seen. It is important to:

GENERAL ALARM
WHEN ALARM SOUNDS
GO TO YOUR STATION
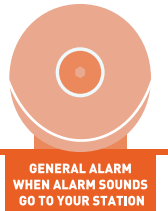
- Sound the emergency alarm and make an announcement that the ship is under attack.
- Conduct exercises prior to entering the area of concern.

Manoeuvring Practice

Where navigationally safe to do so, 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 in getting close enough to execute an attack, without causing a significant reduction in the ship's speed. Anti-piracy manoeuvres are an option when it is navigationally safe to do so.

Closed Circuit Television (CCTV)

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

- Consider positioning CCTV monitors in a protected position.
- Further 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 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.
- Once perpetrators have been identified or an attack commences whilst the ship is underway, illuminating the ship as described above demonstrates to the perpetrators that they have been sighted.
- At anchorage, it is recommended lights are left on as well-lit ships are less likely to be attacked.
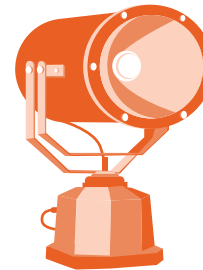
In compliance with international regulation, navigation lights should not be switched off at night.

Deny Use of Ship's Tools and Equipment

Perpetrators generally boarded ships with little in the way of equipment other than 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 that may be of use to the perpetrators should be stored in a secure location.

Safe Muster Points / Citadels

Any decision to evacuate the bridge when 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. An explanation of each follows:

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 will 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 communications such as portable VHF/satellite communications.
- A Safe Muster Point should be located whereby the crew is not visible to the perpetrators and vulnerable to attack.

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 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 is predicated on intervention by maritime enforcement agencies and all persons accounted for.
- Provisions such as food, water, first aid and sanitation should be provided for at least 72 hours.

- The use of 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 is left outside before it is secured.
- The use of a Citadel cannot guarantee a law enforcement/ military response. The crew may have to make a decision to end a Citadel situation without the assistance of law enforcement/military resources.

Additional protection measures may also include:
- Independent tracking system with independent transmitters.
- Motion sensors.
- Door sensors.

ROUTINE SHIP SECURITY REPORTING

The Asian region is bounded by functioning States who apply the rule of law. Also, naval forces operate openly in the region and in close cooperation with each other. The IMO advocates reporting to the nearest coastal States as they have the jurisdiction to respond. It also provides ownership to enforcement in the region and prevention of the maritime crime.

The VCR scheme has been established by the IFC for the purpose of enhancing maritime security for all merchant ships operating in the IFC's VRA.

Merchant ships operating in the VRA are strongly encouraged to report 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 within the military and maritime enforcement agencies.

In return, IFC provides maritime security advisories to ships based on their reported position and intended destinations where applicable and appropriate. IFC will evaluate and monitor selected ships, sharing 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 B** for more details on the VCR scheme.

In the event of an attack, the procedure detailed in Section 10 should be strictly followed.

SHIPS UNDER ATTACK

A. IMMEDIATE ACTIONS

If the crew of a ship suspects a robbery or attack is imminent or in progress there are a number of actions that may be taken. However, the majority of attacks in the region are conducted from small boats, at night and against stationary ships, and potential for the attackers to get close to a ship prior to detection by the crew is high.

A ship could quickly come under attack with little or no warning. This reinforces the need for vigilant lookouts, both visual and radar, to exploit the time taken for the attackers to approach a ship. The time taken to approach a ship, however short, is an important period to activate any protective measures and make it clear to the attackers they have been seen, the ship is prepared and will resist attempts to board.

In the event of an attack, the ship should activate the SSAS and additionally raise the alarm by calling the nearest coastal state through its Maritime Rescue Coordination Centre (MRCC) and IMB. Maintain contact with authorities preferably by telephone for as long as it is safe to do so.

On receipt of information in relation to an attack, the MRCC will inform the regional security forces and ReCAAP Focal Point. IMB will also inform the appropriate national maritime operations centre and local authorities and will alert other ships in the immediate vicinity of the event.

The crew should implement the Company's security plan which is recommended to include a detailed list of actions to be taken. The following list of actions is among those which should be considered by the Master if a suspected attack is imminent or an actual attack is in progress:
- Sound alarm which signals an attack.
- Activate the SSAS which will alert your CSO and Flag State.
- Make an announcement in accordance with the Ship's Emergency Plan.
- The crew will then muster 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.

- Put out a distress alert.
- Ensure that the AIS is switched ON.
- Procedures should be in place to ensure safety of the crew.
- Confirm designated entry point to the accommodation is fully secured.
- Speed should be increased as much as possible to widen the distance between the ship and the attackers. Try to steer a straight course to maintain maximum speed. Consider evasive actions if the circumstances warrant 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 all doors are secured and all crew are mustered within the Safe Muster Point or Citadel. Master to then make the final decision to leave 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, contact IMB by phone and follow up with call to the CSO if the situation permits.

B. INCIDENT REPORTING

Appendix 2 of the IMO circular MSC.1/Circ. 1334 on 'Revised Guidance to ship owner, ship operator, ship master and crew on preventing and suppressing acts of piracy and armed robbery against ships' depicts the information sharing and incident reporting processes in the Asian region (**Annex C**). In the event of an attempted attack or an actual attack, the Master should alert:

I.   The nearest coastal State through its MRCC
II.   the CSO
III. the IMB

The information of MRCC is available in the Admiralty List of Radio Signals Maritime Radio, The Mariner's handbook and Search and Rescue Contacts. Ship master is advised to have the updated list readily available onboard.

You may refer to the following websites for more information:

I.   NP281 Admiralty List of Radio Signals Maritime Radio Stations Europe, Africa and Asia 2015/16 Ed
II.   NP 100 The Mariner's Handbook
III. Search and Rescue Contacts

The CSO should alert:
I.   The Flag State
II.   ReCAAP Focal Point (Refer to **Annex D**)

And if possible alert:
I.   IFC

ACTIONS FOLLOWING BOARDING

Although rare, there have been a limited number of cases in which pirates and armed robbers operating in Asia have used violence in order to subdue the crew. Therefore it is extremely important not to engage in a confrontation with the attackers because this may put the crew at greater risk of getting hurt or in extreme cases killed. Therefore:

- Remain calm. Offer no resistance once attackers reach the bridge. Compliance to attackers is essential once a ship has been taken. They may be aggressive, highly agitated and armed. When directed, all movement should be calm, slow and very deliberate. Crew should keep their hands visible at all times and comply fully. This will greatly reduce the risk of violence.
- If the bridge/engine room is to be evacuated, the main engine should be stopped and all way must be taken off the ship if possible (and if navigationally safe to do so).

Past incidents have shown that attackers will board a ship and loot the ship's stores and steal the crew's personal belongings, but fortunately, kidnappings are rare. However, each company or organisation should have a policy in place to cover the eventualities of kidnap.

In the event that enforcement agencies take action 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 personnel make movements which 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 ship's personnel to cooperate fully during any enforcement agency action on board and prepare them to be challenged on their identity.

PRESERVING EVIDENCE

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

By following some basic principles, the Master and Crew can 'protect' a crime scene until the appointed law enforcement agency arrives:

- Preserve the crime scene and all possible evidence as far as possible.
- Avoid contaminating or interfering with all possible evidence – if in doubt, do not touch and leave items in situ.
- Do not clean up 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.
- Make a list of items taken (eg. 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.

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

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

Tools used by perpetrators
(Courtesy of MMEA)

Tools used by perpetrators
(Courtesy of MMEA)
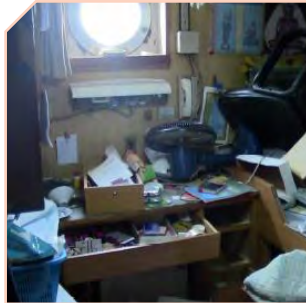
Officer cabin being ransacked
(Courtesy of MMEA)

Footprint on deck
(Courtesy of Thome Ship Management Pte Ltd)

Hand-made cigarette bottle used by perpetrators *(Courtesy of ReCAAP Focal Point (Vietnam))*
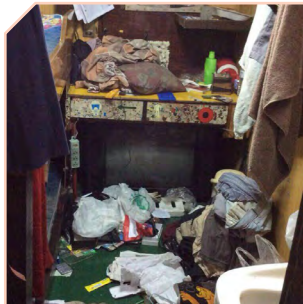
Ransack of crew cabin
(Courtesy of ReCAAP Focal Point (Thailand))

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

Following an incident, a witness statement from those affected is required. Seafarers are encouraged to provide witness statements to Naval/Military forces or law enforcement officers as appropriate to enable suspects to be held and handed over to prosecuting states. Without supporting evidence, including witness statements from those affected by the incident, suspects are likely to go free.

INTERPOL can provide support to ship operators who have had their ships hijacked. INTERPOL's Maritime Security Unit 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 agents pursuing an investigation.

POST-INCIDENT REPORTING

Following an attack, it is vital that a detailed report of the event is provided to:

Flag State
Individual Flag States 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 event is provided to the ReCAAP Focal Points, IFC and IMB. This will enhance knowledge of activity in the maritime domain and better tailor future warnings or advice the regional reporting centres issue to the maritime community. The report should follow the format contained in the **Annex E** to this Guidance (for contact details, see **Annex D**).

Coastal States
It is essential that each and every incident is reported to the relevant coastal state to assist them in fulfilling their obligations under UNCLOS 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 Vessel Traffic Information System (VTIS) and have 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.

OTHER CONSIDERATIONS

Companies should consider helping the crew overcome trauma of attack. There are a number of international programmes run by NGOs available who can provide advice on the after-care and support of seafarers.

Piracy, in accordance with Article 101 of the United Nations Convention on the Law of the Sea (UNCLOS), is defined as:

1. "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).

Armed Robbery Against Ships, in accordance with 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), is defined as:

2. "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

The VCR merchant ship voluntary reporting schemes as depicted on 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's VRA.

Merchant ships operating in the VCR region are strongly encouraged to report maritime security incidents or anomalous behaviour to the IFC. 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 risk evaluate and monitor selected ships, sharing the information with other maritime enforcement agencies when required. Ships are encouraged to report under the following conditions:

   A.   When transiting in Southeast Asia.
   B.   Any items changed from the initial report.
   C.   On the occurrence of a maritime security incident.
   D.   Observing any suspicious or anomalous behaviour.

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 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 nav 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
- Ships underway/making way without AIS transmission

It is recommended that the VCR reports consist of the following fields of information and be sent to information_fusion_centre@defence.gov.sg.

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
14	Company (Contact Details and Email)

Daily Position Report	
01	Ship Name
02	International Radio Call Sign (IRCS)
03	IMO Number
04	Time of Report (UTC)
05	Ship Position
06	Course / Speed
07	Any Other Important Information
08	Company

Final Report	
01	Ship Name
02	International Radio Call Sign (IRCS)
03	IMO Number
04	Time of Report (UTC)
05	Port or Position
06	Company

Suspicious Activity Report	
01	Ship Name
02	IMO Number
03	Type of suspicious activity
04	Position of incident
05	Details of incident
06	Inmarsat number
07	Email address to be contacted by
08	Date and Time of report (at GMT)
09	Company

IFC VOLUNTARY REPORTING AREA

(Area as marked on Marsec Charts Q6112 and Q6113)
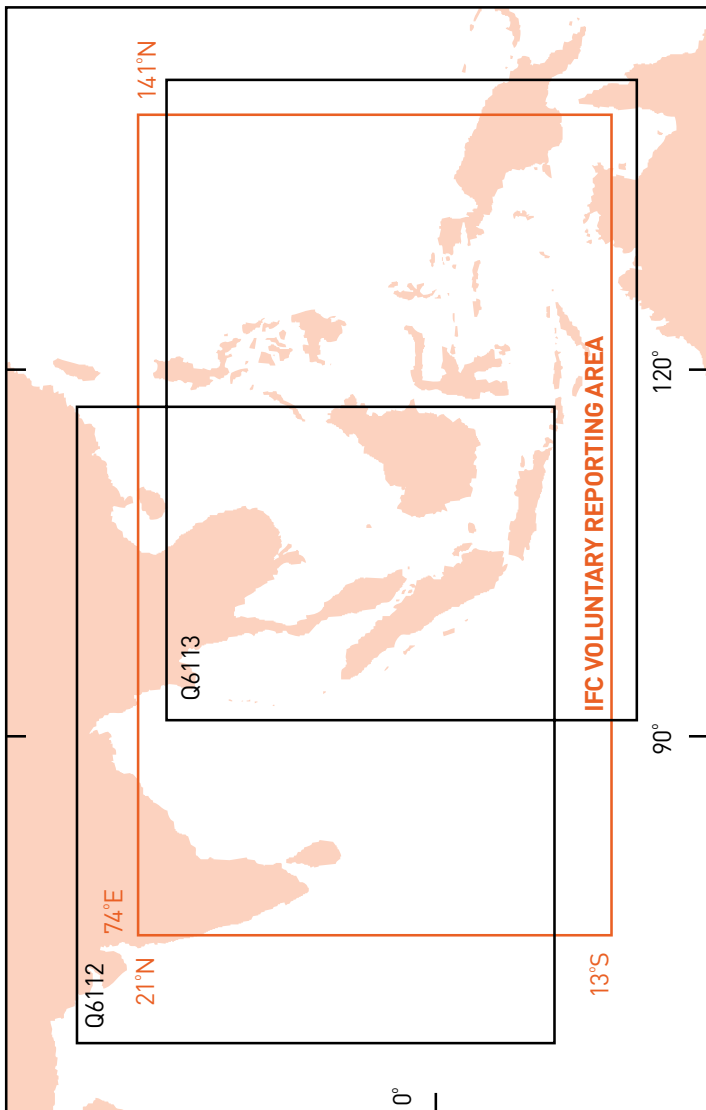
IMO CIRCULAR

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 to the nearest coastal States as advocated by the IMO circular MSC.1/Circ. 1334 on 'Revised Guidance to ship owner, ship operator, ship master and crew on preventing and suppressing acts of piracy and armed robbery against ships'. Refer to Appendix 2 of the circular on the flow diagram for reporting incidents in Asia on page 43.

Diagram I: Flow Diagram for Reporting Incidents in Asia

Legend
— Radio/GMDSS
--- Fastest means, not radio
···· Follow-up by letter, fax or email
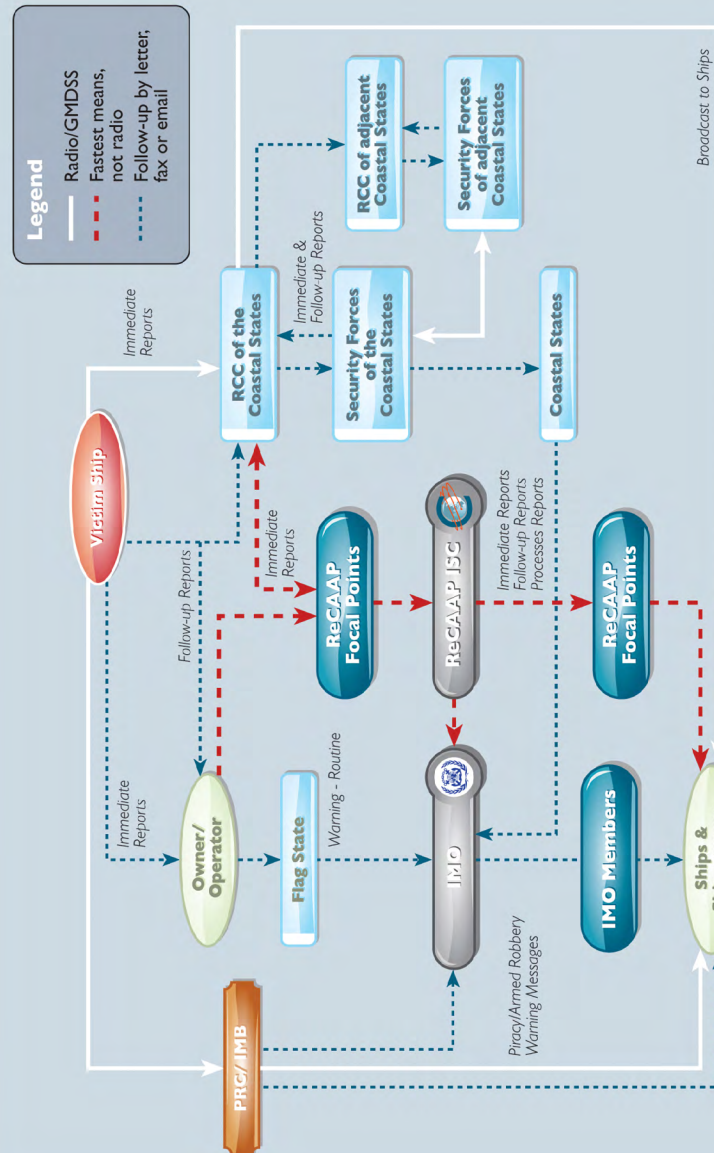
CONTACT DETAILS

Country & Agency In Charge	Point of Contact	
	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
China (ReCAAP Focal Point)		
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 (ReCAAP Focal Point)		
Danish Maritime Authority (DMA) Email: ReCAAP-FP-DK@dma.dk	+45-9137-6000	+45-9137-6001

Country & Agency In Charge	Point of Contact	
	Phone No	Fax Number
India (ReCAAP Focal Point)		
MRCC (Mumbai) Coast Guard Region (West) Mumbai – India Email: indsar@vsnl.net icgmrcc_mumbai@mtnl.net.in mrcc-west@indiancoastguard.nic.in	+91-22-2431-6558 +91-22-2438-8065	+91-22-2433-3727 +91-22-2431-6558
Indonesia		
Badan Keamanan Laut Republic Indonesia (BAKAMLA) www.bakamla.go.id	021 - 1500500 021 - 127	
Japan (ReCAAP Focal Point)		
Japan Coast Guard (JCG) Ops Centre Email : jcg-op@mlit.go.jp	+81-3-3591-9812 +81-3-3591-6361	+81-3-3581-2853
Republic of Korea (ReCAAP Focal Point)		
Ministry of Oceans and Fisheries Operations Centre Email: piracy@gicoms.go.kr	+82-44-200-5895 to 98	+82-44-200-5886 to 88
Laos (ReCAAP Focal Point)		
International Relation Department Ministry of Public Security Email: keo_kkk@hotmail.com	+85-6-2121-2505	+85-6-2121-2505 +85-6-2121-2547
Malaysia		
Malaysian Maritime Enforcement Agency (MMEA) www.mmea.gov.my		
Northern Region	604-9669800	604-9660542
Southern Region	607-2199400	607-2236101
Eastern Region	609-5717300	609-5733569
Sabah Region	608-838 5000 608-8524600	608-838 4161
Sarawak Region	608-2432553 608-2432544	608-2432502

Country & Agency In Charge	Point of Contact	
	Phone No	Fax Number
Myanmar (ReCAAP Focal Point)		
MRCC Ayeyarwaddy (Myanmar Navy) Email: mrcc.yangon@mptmail.com.mm	+95-313-1650	+95-1202-417
Netherlands (ReCAAP Focal Point)		
Dutch Coastguard Maritime Information Centre (MIK-NL) Email: mik-nl@kustwacht.nl	+31-223-658-382	+31-223-658-358
Norway (ReCAAP Focal Point)		
Norwegian Maritime Authority Email: morten.alsaker.lossius@sjofartsdir.no	+47-5274-5000 +47-5274-5130	+47-5274-5001
Philippines (ReCAAP Focal Point)		
Philippine Coast Guard PCG Action Centre-MRCC (Manila) Email: pcg_cg2@yahoo.com cg2@coastguard.gov.ph isc.cg2@coastguard.gov.ph	+63-2-527-3877 +63-2-527-8481 to 89 (ext: 6136/6137) +63-917-724-3682 (Text Hotline) +63-2-527-8481 loc6122	+63-2-527-3877
Singapore (ReCAAP Focal Point)		
Maritime and Port Authority of Singapore Port Operations Control Centre (POCC) Email: pocc@mpa.gov.sg	+65-6226-5539 65-6325-2493	+65-6227-9971 +65-6224-5776
Sri Lanka (ReCAAP Focal Point)		
Sri Lanka Navy Operations Room / MRCC (Colombo) Email: nhqdno@navy.lk nhqdno@yahoo.com	+94-11-244 5368	+94-11-244 9718
Thailand (ReCAAP Focal Point)		
Royal Thai Navy Maritime Information Sharing Centre (MISC) Email: miscdutyofficer@misc.go.th	+66-2475-4532	+66-2475-4577

Country & Agency In Charge	Point of Contact	
	Phone No	Fax Number
United Kingdom (ReCAAP Focal Point)		
National Maritime Information Centre Operations Centre Email: nmic-group@mod.uk	+44 2392-211951	+44 2392-212024 Please indicate ˝FAO NMIC – A leg˝ if send via fax
United States (ReCAAP Focal Point)		
USCG Rescue Coordination Center Alameda (RCCAlameda) Email: rccalameda@uscg.mil	+1-510-437-3701	
Vietnam (ReCAAP Focal Point)		
Vietnam Coast Guard Email: vietnamcoastguard@gmail.com vietnamfocalpoint@yahoo.com.vn	+84-4-3355-4378	+84-4-3355-4378
Information Fusion Centre (IFC)		
Information Fusion Centre (IFC) Email: ifc_do@defence.gov.sg	65-6594-5728 (During office hours) +65-9626-8965 (After office hours)	+65-6594-5734
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 5769

(Please refer to the ReCAAP ISC Mobile App for the updated contact details of the ReCAAP Focal Points and Contact Point.)

▬ ReCAAP Focal Points   ▬ Other Agencies

Correct as at 16 February 2016

PIRACY ATTACK REPORT
•••

Following any attack or sighting of suspicious activity, it is vital that a detailed report of the event is sent to IMB, ReCAAP and/or IFC via e-mail or fax. The appropriate and relevant information from an incident will be used to support INTERPOL and regional law enforcement investigations.

ATTACK REPORT SHIP PARTICULARS/DETAILS

General Details	
01	Ship Name
02	IMO No
03	Type of Ship
04	Flag
05	Gross Tonnage
06	Date and Time
07	Latitude / Longtitude
08	Name of the area
09	While sailing, at anchor or at berth?
10	Method of attack
11	Description / Number of suspect craft
12	Number and brief description of pirates/robbers
13	What kind of weapons did the pirates/robbers carry?
14	Any other information (e.g., language spoken)
15	Injuries to crew and passengers
16	Damage to ship (Which part of the ship was attacked?)
17	Brief details of stolen property/cargo
18	Action taken by the master and crew
19	Was incident reported to the coastal authority and to whom?
20	Reporting State or international organisation
21	Action taken by the coastal State

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, 20 States have become Contracting Parties to ReCAAP.

The 20 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 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 Unites 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 Information Network System (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.
www.recaap.org

IFC

The Information Fusion Centre or IFC is a 24/7 regional Maritime Security (MARSEC) information-sharing centre. 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, we facilitate timely responses with our partner countries on maritime incidents. We also aim 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 65 agencies in 35 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. The Voluntary Community Reporting (VCR) is one of the initiatives by IFC to engage the shipping community through information sharing and reporting. In return, IFC shares shipping advisories to the VCR members through its weekly reports, monthly maps and SMS alerts warning mariners about the situation at sea. 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 Programme (RMPP). The IFC also hosts maritime information sharing portals such as the ASEAN Information Sharing Portal and the Regional Maritime Information exchange (ReMIX), which facilitates information sharing among ASEAN navies and Western Pacific Naval Symposium members.
www.infofusioncentre.gov.sg

RSIS

The S. Rajaratnam School of International Studies (RSIS) was established in January 2007 as an autonomous School within the Nanyang Technological University. Known earlier as the Institute of Defence and Strategic Studies when it was established in July 1996, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific.

RSIS offers a challenging graduate education in international affairs through its five Masters programmes, taught by an international faculty of leading thinkers and practitioners. A small but select PhD programme caters to advanced students who are supervised by faculty members with matching interests.

Research takes place within RSIS' five components: the Institute of Defence and Strategic Studies (IDSS, 1996), the International Centre for Political Violence and Terrorism Research (ICPVTR, 2004), the Centre of Excellence for National Security (CENS, 2006), the Centre for Non-Traditional Security Studies (Centre for NTS Studies, 2008); and the Centre for Multilateralism Studies (CMS, 2011). The focus of research is on issues relating to the security and stability of the Asia Pacific region and their implications for Singapore and other countries in the region.

Collaboration with other professional schools of international affairs to form a global network of excellence is a RSIS priority. RSIS maintains links with other like-minded schools so as to enrich its research and teaching activities as well as adopt the best practices of successful schools.
www.rsis.edu.sg

ReCAAP FOCAL POINTS / CONTACT POINT

ReCAAP Contracting Parties	Designated Agencies as Focal Points
Australia	Maritime Border Command (MBC)
Bangladesh	Department of Shipping
Brunei	National Maritime Coordination Centre
Cambodia	Merchant Marine Department
China	China Maritime Search and Rescue Centre (Beijing)
	Maritime Rescue Coordination Centre (Hong Kong)
Denmark	Danish Maritime Authority (DMA)
India	Indian Coast Guard (ICG)
Japan	Japan Coast Guard (JCG)
Republic of Korea	Ministry of Oceans and Fisheries
Laos	Ministry of Public Security
Myanmar	Myanmar Navy
Netherlands	Netherlands Coastguard
Norway	Norwegian Maritime Authority
Philippines	Philippines Coast Guard (PCG)
Singapore	Maritime and Port Authority of Singapore (MPA)
Sri Lank	Sri Lanka Navy
Thailand	Royal Thai Navy (RTN)
United Kingdom	National Maritime Information Centre (NMIC)
United States	US Coast Guard
Vietnam	Vietnam Coast Guard (VCG)

ASF

The Asian Shipowners' Forum (ASF) was founded in April 1992. There are eight members of the ASF, being the shipowner associations of Australia, China, Hong Kong, India, Japan, Korea, Chinese Taipei and the Federation of ASEAN Shipowners' Associations (FASA), consisting of Brunei, Indonesia, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. The ASF membership is estimated to control about 50% of the world merchant fleet.

There are five standing committees of the ASF. These are the Seafarers Committee (SC), Shipping Economics Review Committee (SERC), Ship Insurance & Liability Committee (SILC), Safe Navigation & Environment Committee (SNEC) and Ship Recycling committee (SRC).

In view of the growing importance of the ASF, a secretariat office was opened in Singapore in November 2007. The ASF office acts as a channel to convey Asian Shipowners' voices to the international shipping community as well as to enhance and strengthen the ASF's stature. At the same time, it is also a platform for all ASF members to liaise with one another and to help promote cooperation, amity and friendship amongst its members.
www.asianshipowners.org

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.
www.fasa.org.sg

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.
www.intertanko.com

OCIMF

Oil Companies International Marine Forum (OCIMF) is a voluntary association of oil companies having an interest in the shipment and terminalling of crude oil and oil products. Our mission is to be the foremost authority on the safe and environmentally responsible operation of oil tankers, terminals and offshore support ships, promoting continuous improvement in standards of design and operation.
www.ocimf.org

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.
www.ssa.org.sg

SUPPORTING ORGANISATIONS:

INTERPOL

INTERPOL is the world's largest international police organization, with 190 member countries. Created in 1923, it facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime. INTERPOL's Maritime Security Unit (MTS) was set up in January 2010 to co-ordinate the Organization's international response to the maritime piracy threat in its various facets by:

- Improving the global collection, preservation, analysis and dissemination of piracy-related evidence and intelligence in aid of criminal investigations and prosecutions by its member countries; and
- Developing police and judicial investigative and prosecution capabilities in Eastern Africa in partnership with key international actors and donors.

www.interpol.int

MMEA

Malaysian Maritime Enforcement Agency (MMEA) is the sole maritime law enforcement agency in Malaysia established under the the enactment of the Malaysian Maritime Enforcement Agency Act 2004 (Act 633) by the Malaysian Parliament in May 2004. The roles & functions of MMEA includes enforce law & order under any federal law in the Malaysian Maritime Zone; conduct & coordinate maritime search & rescue; prevent & suppress the commission of an offence; lend assistance in any criminal matters on request by a foreign state (mutual assistance act 2002); carry out air & coastal surveillance; provide platform services to any relevant agency; to ensure maritime security and safety; control and prevention of maritime pollution in the sea; prevent and suppress piracy and illicit trafficking of narcotic drug on the high sea. During period of emergency MMEA will be placed under the control of the Malaysian Armed Forces.

www.mmea.gov.my

SSSA

90% of the transportation for East and West Malaysia depending on Sea transport. In order to gather and unite all the Shipowner in Sibu, "Sarawak United Coastal Shipowner Association" was established in 6th May 1979 for these purposes. The demand of shipping in Sarawak continues increase and demand more seafarers, the Association appealed to Marine Department for conducting more marine modular courses and relevant examinations to train and establish more capable local seafarers. In 1981, the Association rename to "Sibu Coastal Shipowner Association" and continue to serve the shipping community in Sibu.

Over the past 35 years, the Association has continuously organized dialog, seminar and training. In year 2014, we celebrated 35th Anniversary and publish the 2nd commemorative magazine. We will continue to voice out the needs of members, such as ship registration, ship survey, fuel subsidies, insurance privileges and also assist with any problems from shipping community. The association acts as bridge between shipowner and government to co-ordinate, develop and promote shipping and marine services.

Due to the over whelming respond from Shipowners in Sabah and Sarawak, the Association is renamed to "Sarawak and Sabah Shipowner Association" in 6th May 2010. Currently, we have more than 130 registered members and there are more than 2,500 ships under members' fleet.

In order to allow member to gain more knowledge and assess into latest maritime news, we established a website launching in 2011 and we started to accept associate member such as maritime-related companies, schools, individuals and association to join us as associate member. In the future, we hope to work hand in hand with Shipowners and continue our service to the shipping community.

www.sssa.org.my

LIST OF ABBREVIATIONS AND ACRONYMS

AIS	Automatic Identification System
CSO	Company Security Officer
IMB	International Maritime Bureau
IMO	International Maritime Organization
ISPS	International Ship and Port Facility Security
MRCC	Maritime Rescue Coordination Centre
NUC	Not Under Command
PCASP	Private Contracted Armed Security Personnel
PMSCs	Private Maritime Security Contractors
SBM	Single Buoy Mooring
SOMS	Straits of Malacca and Singapore
SSA	Ship Security Assessment
SSAS	Ship Security Alert System
SSO	Ship Security Officer
SSP	Ship Security Plan
STS	Ship to Ship
TaB Guide	Tugs and Barges Guide
UNCLOS	1982 UN Convention on the Law of the Sea
VCR	Voluntary Community Reporting
VRA	Voluntary Reporting Area
VTIS	Vessel Traffic Information System

NOTE

NOTE

NOTE

Regional Cooperation Agreement on Combating Piracy and Armed Robbery against 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