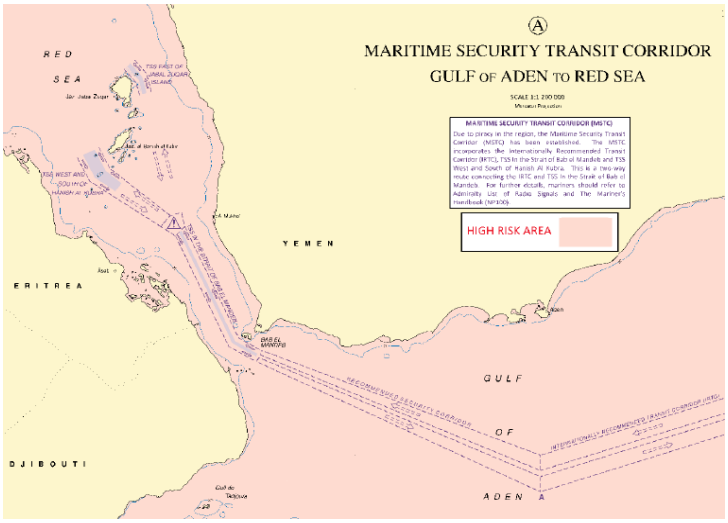
Interim Guidance on Maritime Security in the Southern Red Sea and Bab al-Mandeb

To be read in conjunction with BMP 4



Produced by:

BIMCO

International Chamber of Shipping

INTERTANKO

Supported by:

IGP&I

Background

The conflict in Yemen has introduced additional maritime security threats, other than piracy, to the Southern Red Sea and Bab al-Mandeb; these include collateral damage due to conflict between groups in the region and a potential deliberate targeting of ships. The guidance contained in this publication is specific to known threats in this particular region.

The purpose of this guidance is to help Company Security Officers (CSOs) and Masters in conducting a threat assessment in respect of transits through the Southern Red Sea and Bab al-Mandeb. Experience has shown awareness of other threats and application of the recommendations contained within this guidance, in conjunction with application of the BMP 4 recommendations, may prevent a successful attack. This guidance is complimentary to and should be applied in conjunction with the application of BMP 4.

The consequences of not adopting effective security measures can be severe.

This guidance relates to information available at the time of writing and does not speculate on any future threats that may emerge due to regional instability. Amended guidance will be provided whenever the situation changes based upon credible threat and risk advice that is endorsed by military forces in the region and flag states. The situation internally in Yemen and within its ports means that perceived non-piracy threats may be reported at short notice, and CSOs and Masters should, therefore, assess the suitability of mitigation measures against more than one type of threat eg piracy.

Threat profile

Military published threat assessments, as well as the threat and risk information provided by flag states, should be consulted regularly in order to fully understand current threats and the likelihood of attack. Risk assessments should take into account the threat level information provided by the flag state.

The level of preparedness that a ship will need to safely transit the areas will be based on a number of ship and voyage specific factors, and should take into account information from the authorities and sources detailed in Annex A.

Whilst BMP measures are effective mitigation against piracy, it should be recognised that other threats may have differences in attack methodology and intent and, may therefore require other forms of mitigation. For example, attacks carried out by non-pirate groups may be more determined, even risking injury or death, and this may diminish the effectiveness of some of the self-protection measures successfully used against pirates in the region.

Maritime security threats

Missiles

Missiles are long range, accurate and powerful weapons and have been used against military ships in the region. Whilst military reports suggest that military ships in the region have been targeted with anti-ship missiles, there is no indication that merchant shipping is likely to be deliberately targeted. There is however a risk of misidentification or collateral damage to merchant shipping and as such it is strongly recommended that ships utilise the Maritime Security Transit Corridor (MSTC) and maintain an awareness of the other vessels around them.

Sea mines

Sea mines have been used to deter and deny Saudi-led coalition forces access to key ports in Yemen's southern Red Sea area. Whilst merchant shipping is not the target, sea mines may affect commercial ships using these ports or routeing close to the Yemeni Coastline. It is strongly recommended that ships utilise the MSTC when transiting through the area to minimise the threat from sea mines.

Water-Borne Improvised Explosive Devices (WBIED)

An attack involving a WBIED is likely to involve one or more skiffs approaching the merchant ship at high speed firing both small arms and Rocket-Propelled Grenades (RPGs). One or more of the boats may be laden with explosives. On the basis of current understanding it is assessed that merchant shipping is unlikely to be directly targeted by a WBIED, however the risk of collateral damage or misidentification remains. Counter-piracy mitigation measures contained in BMP including, but not limited to, increasing speed, manoeuvring, etc., should be applied to prevent the skiffs from attaching to or making contact with the ship's hull. Information on changes in modus operandi in WBIED tactics will be provided in the Industry Releasable Threat Bulletins (IRTBs) regularly disseminated by Maritime Security Centre Horn of Africa (MSCHOA) and the Combined Maritime Forces (CMF). United Kingdom Maritime Trade Operations (UKMTO) Navigational Warnings (NAVWARNS) will provide immediate information on incidents and threats.

WBIED attacks have been used against Saudi coalition warships and associated assets eg military supply ships in the southern Red Sea.

The MV Muskie (31 May 2017) and MV Galicia Spirit (25 October 2016) incidents, which took place in the southern approaches to the Bab al-Mandeb (BAM), highlight a non-piracy attack by groups operating in Southern Yemen. In these incidents there was an explosion during the approach and, likely attempted boarding respectively. This tactic marked a significant departure from Somali piracy and, other incidents associated with the Yemen conflict, and as such the likely intent and perpetrators are not clear.

Two separate incidents on 6 January 2018, approximately 45 nm off the port of Al Hudaydah, Yemen, involved suspicious approaches to two merchant ships by two speed boats carrying armed personnel with optical equipment and one unmanned boat. After the merchant ships undertook evasive action, the speed boats broke off their approach. The speed boats subsequently approached a tanker under escort and the escort vessel engaged the speed boats and destroyed the unmanned vessel.

Whilst it remains unlikely that merchant shipping will be deliberately targeted, the potential for collateral damage and misidentification remains, and ships are recommended to utilise the MSTC to minimise this risk.

Preparations and self-protection

Companies and ships are strongly advised to consider the following actions and measures to enhance the safety and security of the ship whilst transiting the region, taking into account the guidance in BMP 4.

Obtain information

CMF and European Naval Forces (EUNAVFOR) produce quarterly Industry-Releasable Threat Assessments (IRTA) and IRTBs that provide rapid and responsive information. These will be valuable resources for every risk assessment and are circulated by MSCHOA and the Shipping Industry Associations. CSOs and Masters should obtain the latest information from CMF, EUNAVFOR and the UKMTO and other relevant organisations (see Annex A), and contact the ship's flag state for guidance on the threat level and any necessary actions to be taken in accordance with the requirements of the International Ship and Port Facility Security Code (ISPS).

Review existing plans

The CSO and Master should review the threat/risk assessments and update plans as necessary; including the Ship Security Assessment (SSA), Ship Security Plan (SSP) and Vessel Hardening Plans (VHP) and implement any new measures.

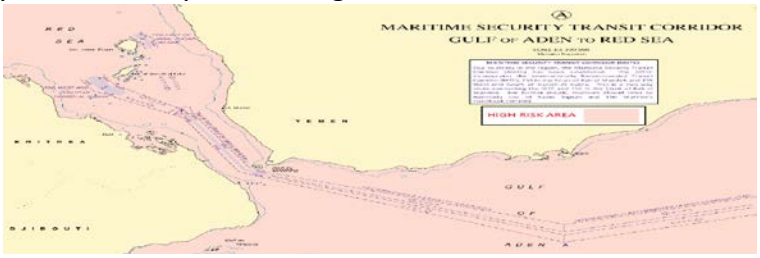
Register with MSCHOA and report to UKMTO

It is essential that ships should register with MSCHOA and report to UKMTO to ensure that the military is aware of their presence in the region and to give the ship access to information and support from military forces in the region.

Use the Maritime Security Transit Corridor (MSTC)

The MSTC is a military established corridor upon which naval forces focus their presence and surveillance efforts. The MSTC consists of:

- The Internationally Recommended Transit Corridor (IRTC)
- The Bab al-Mandeb (BAM) Traffic Separation Scheme (TSS) and the TSS West of the Hanish Islands
- A two-way route directly connecting the IRTC and the BAM TSS.



It is strongly recommended that ships use the MSTC to gain the maximum benefit from military presence and surveillance (refer to Chart Q6099 for details).

Privately Contracted Armed Security Personnel (PCASP)

Attention is drawn to the difficulty in differentiating between a non-piracy attack and a piracy attack, as this may not be possible until analysis after any incident. The use of PCASP to deter a non-piracy related attack may not be permitted under some jurisdictions. The CSO should gain clarity from the ship's the flag state on its policy concerning the use of PCASP under such circumstances, particularly with respect to the escalation to the use of lethal force.

Protection against explosions

The CSO in conjunction with the Master should decide upon and designate a safe location for the crew in the event of a threat of an external explosion. Thought should be given to blast routes that will help channel the main force of any blast away from the safe muster area. In many ships, the central stairway may provide a safe location due to the greater protection being afforded by the accommodation block and being well above the waterline. Consideration should be given in the risk assessment and planning to the circumstances, under which the crew would be directed to a safe muster area, recognising that piracy and non-piracy related attacks may look similar in the initial stages.

Reporting suspicious activity to UKMTO and MSCHOA

UKMTO advises on the types of activity of interest to the regional maritime security community utilising information from "Piracy Attack / Suspicious Activity Reports" (Annex B). UKMTO can forward information received in an anonymised form to the most appropriate agency empowered to act. While suspicious activity may appear inconsequential in isolation, when added to other reports it may actually prove to be extremely valuable.

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

Annex A

Contact details

Emergency contacts:

UKMTO (United Kingdom Maritime Trade Operations)

Email:	watchkeepers@ukmto.org
Tel:	+44 2392 222060
	+971 50 552 3215

MSCHOA

Email	postmaster@mschoa.org
Tel	+44 (0)1923 958 545
Fax	+44 (0)1923 958 520
Website	www.mschoa.org

USN Naval Control and Guidance to Shipping

Email	CTF55.BWC@me.navy.mil
Tel (24hrs)	+ 973-1785-3434

Other useful contacts

NATO Shipping Centre

Email	info@shipping.nato.int
Tel	+44 (0)1923 956 574
Fax	+44 (0)1923 956 575
Website	www.shipping.nato.int

IMB Piracy Reporting Centre

Email	piracy@icc-ccs.org
	imbkl@icc-ccs.org
Tel	+603 2031 0014 (24hr Helpline)
Fax	+603 2078 5769
Website	www.icc-ccs.org

Annex B

UKMTO Piracy Attack / Suspicious Activity Report

General Details

01	Name of Ship:	
02	IMO No:	
03	Flag:	
04	Call Sign:	
05	Type of Ship:	
06	Tonnages: NRT:	GRT: DWT:
07	Owner's (Address & Contact Details):	
08	Manager's (Address & Contact Details):	
09	Last Port/Next Port:	
10	Cargo Details: (Type/Quantity)	

Details of Incident

11	Date & Time of Incident: LT UTC
12	Position: Lat: (N/S) Long: (E/W)
13	Nearest Land Mark/Location:
14	Port/Town/Anchorage Area:
15	Country/Nearest Country:
16	Status (Berth/Anchored/Steaming):
17	Own Ship's Speed:
18	Ship's Freeboard During Attack:
19	Weather During Attack (Rain/Fog/Mist/Clear/etc, Wind (Speed and Direction), Sea/Swell Height):
20	Types of Attack (Boarded/Attempted):
21	Consequences for Crew, Ship and Cargo: Any Crew Injured/Killed: Items/Cash Stolen:
22	Area of the Ship being Attacked:
23	Last Observed Movements of Pirates/Suspect Craft:
24	Type of vessel (Whaler, Dhow, Fishing Vessel, Merchant Vessel)
25	Description of vessel (Colour, Name, Distinguishing Features)
26	Course and Speed of vessel when sighted

Details of Raiding Party

27	Number of Pirates/Robbers:
28	Dress/Physical Appearance:
29	Language Spoken:
30	Weapons Used:
31	Distinctive Details:
32	Craft Used:
33	Method of Approach:
34	Duration of Attack:
35	Aggressive/Violent:

Further Details

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