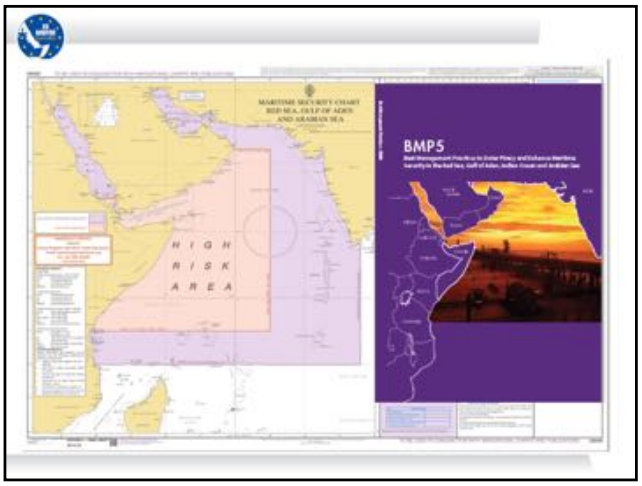


Thank you for the opportunity to speak to you about the role of the Maritime Security Centre Horn of Africa, MSCHOA, for shipping in the region.
So what is MSCHOA, what information is shared, and why?

Firstly, it is important to note that the Maritime Security Centre Horn of Africa (MSCHOA) sits inside the EU NAVFOR Headquarter in Northwood. While a civilian entity with a separate legal identity, it is part and parcel of the operation, with direct links to the 'CJ3 cell' – the current operations branch of EU NAVFOR – and with immediate access to EU NAVFOR's command group.

In case of incidents, we like to see the chain as FIND – FIX – FINISH – EXPLOIT – ANALYSE
In case of piracy, MSCHOA coordinates and ensures the Find – fix – finish parts of this.
In case of non-piracy incidents, MSCHOA ensures the Find & fix parts, and then hands off the case to others for the legal finish.

So what information is shared with MSCHOA, and why?
When piracy spiralled out of control in 2008-2009 and military responses were set up, we had an honest conversation with the shipping industry. Essentially, we said: "There is only one way of providing protection in an area this size, and that's by you agreeing to introduce specific instructions to your ships to transmit commercially confidential information to EU NAVFOR so that we can assess the risk, provide you

with advice, and respond properly in case of an attack."
So to this day, about 5,000 ships report to MSCHOA every month, informing us of their route, their speed, their self-protection measures, their cargo, and their protocols. There is no legal requirement for them to do this, and it is highly sensitive information. So the only reason they are willing to do this, is that we provide them with timely information and a guaranteed response. If you report you are attacked, we will coordinate a response, as we are the conduit for a naval military response. Take away the response, take away the naval military presence, and we become merely a depository for information and ships no longer have the incentive to report and self-protect.

FOUO – For Official Use Only

Industry Releasable Threat Bulletin (IRTB) 011 (to IRTA 1 Sept 18)

Issued: 19 Oct 18

For official use only. This Threat Bulletin has been released to the Shipping Industry in confidence. It should not be disseminated further without permission.

1. **Foreword.** This IRTB has been written by European Union Naval Forces (EU NAVFOR) and Combined Maritime Forces (CMF). It is intended to inform risk management decision making for shipping operators responsible for merchant vessels that are transiting through the Red Sea, Gulf of Aden (GoA), Gulf of Oman (GoO) and the Wiestern Indian Ocean.

2. **Purpose.** The purpose of an **Industry Releasable Threat Bulletin (IRTB)** is to provide a specific update to industry on events that may require an interim update to the most recent Industry Releasable Threat Assessment (IRTA). The information contained in the IRTBs will be incorporated into the next IRTA.

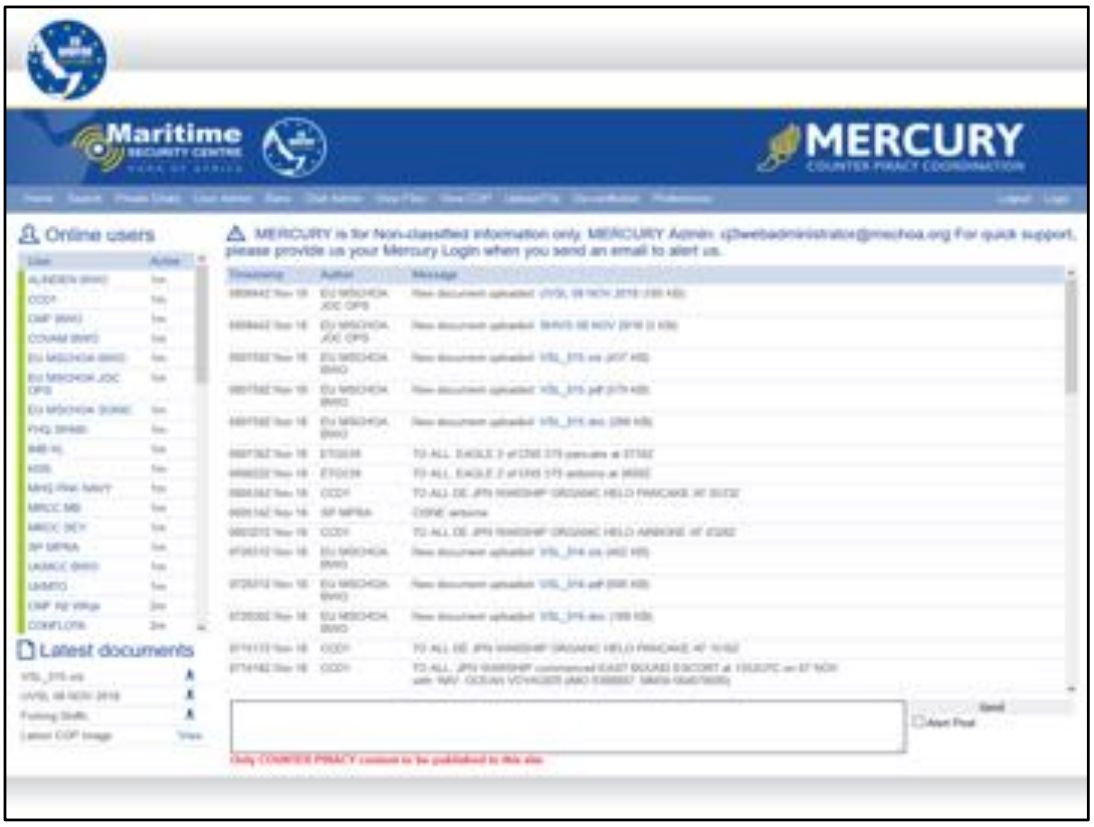
3. **Incident/Identifier.** Reported attack on Hong Kong (HK) flagged bulk carrier in the Somali Basin (SB).

4. **Date/time.** 16 1234 UTC Oct 18.

5. **Location.** Indian Ocean, Somali Basin, approximately 400 NM E of Baardwe and 340 NM SE of Mogadishu, Somalia, in position 00 49 00N – 050 53 00E.

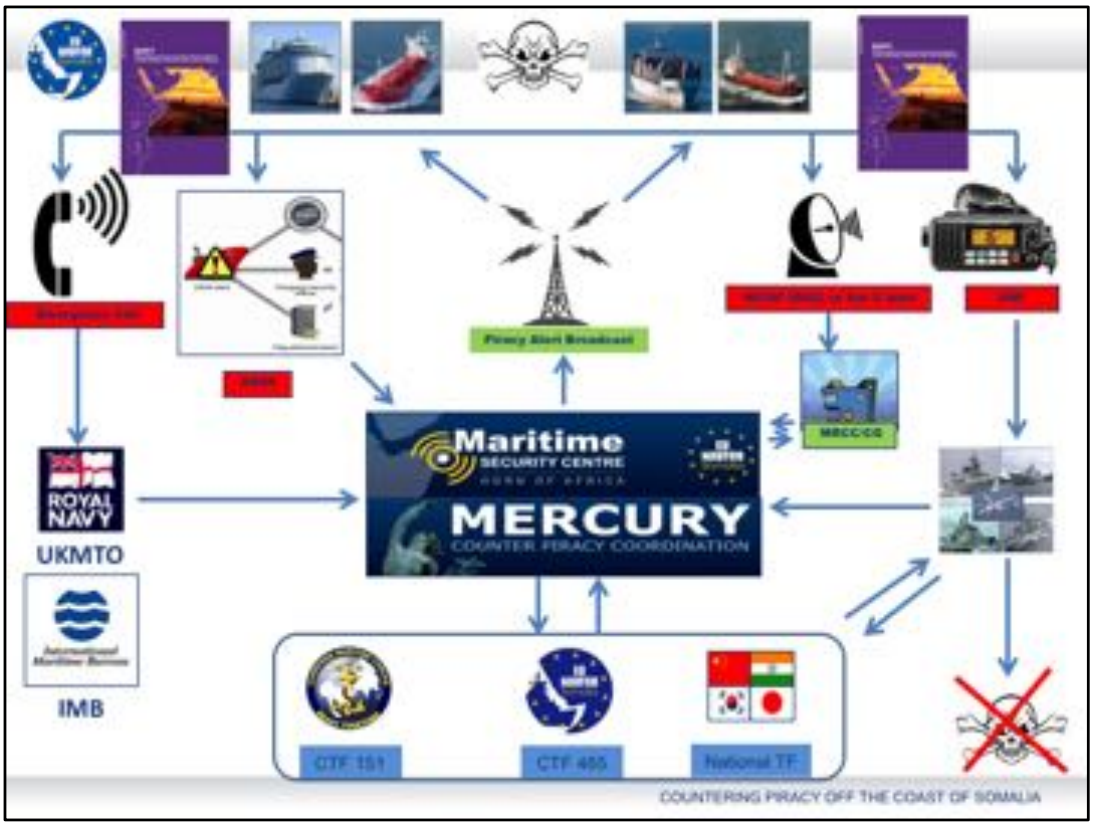
So as I indicated, MSCHOA sends out a specific 'IRTB' in case of an incident. It is sent out to everyone signed up to the system, with a total of XXX people receiving it. This ranges from Masters of vessels, to military actors, to local security actors, to diplomats in the region. It presents the issue at hand, followed by a detailed description, outcome, follow-up, assessment and recommendations.

So this is after the incident, and after the FIND – FIX – FINISH has taken place, where we provide the EXPLOIT and ANALYZE phase.



The IRTA and IRTB are in addition to the Mercury system, which is the sharing information tool, MSCHOAs 'chat room' that connects military actors and government entities. On this chat, the military actors report where they are and what their activities are that day, for instance concerning planes or helicopters flying.

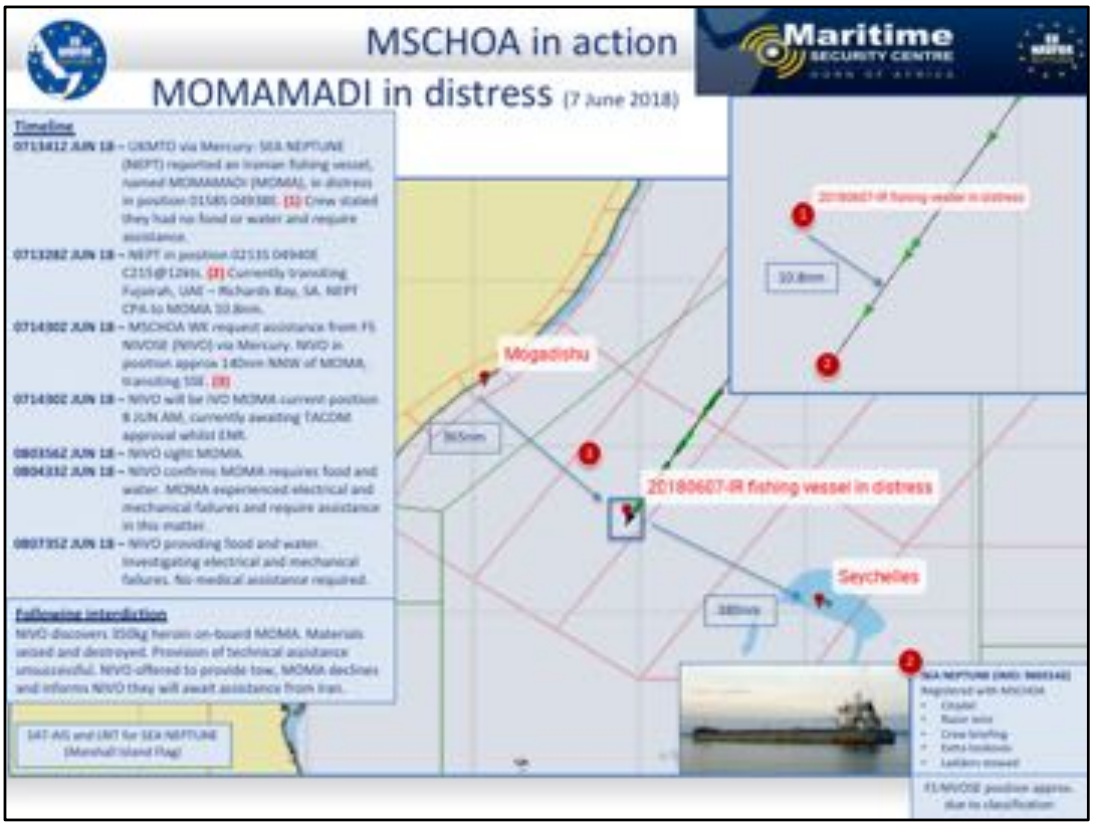
I'll give you an example of how this helps us in practice. After the KSL Sydney reported to be under attack from pirates in mid-October, we reported this on Mercury. At this time, the Seychellois were patrolling with their aircraft. Seychelles MRCC noticed the post and offered to send its aircraft to the region to patrol. In the meantime, MSCHOA was in touch with ACE, the air coordination element in Bahrain to ensure deconfliction between EU NAVFOR, CMF, and other military aircraft in the region.



So how this works in practice then, is that a ship calls in an incident to the 'emergency room', or 911 call, to UKMTO or IMB. They report to us, and we coordinate with ships, Task Forces, send out a piracy alert and coordinate with flagstates and security actors. MSCHOA itself plays the role of coordinator. While available 24/7, 365 days of the year, it plays a much broader role than just the call centre receiving the call from a ship in distress.

So what does it do?

1) In case of an incident, it coordinates the response of the various assets and Task Forces via the Mercury tool;
2) It communicates with the shipping industry to inform them of trends, threats and protection measures;
3) It works with flagstates to ensure ships have the necessary information, and that protocols are in place in case of any incidents.
4) It works with security companies to help them understand where the threats are and how to respond to it.



Here is an example of an Iranian fishing vessel in distress somewhere between Somalia and the Seychelles. The first call is to the UK Maritime Transport Organisation (UKMTO), as that is the 'emergency call centre', or '911' if you like. This was done by a different ship, the MV Sea Neptune. UKMTO then used Mercury to make all aware of the distress, resulting in MSCHOA assessing who is available and coordinating a response, in this case by the French frigate NIVOSE, as it was nearest to the incident. MSCHOA thus provided the FIND and FIX elements of the incident, then handing off the case to a vessel under national tasking when it emerged it was not a piracy incident.

As you can read, water and food was provided, but technical assistance did not help. A tow was offered but declined. But in the process, 350kg of heroin were found, seized and destroyed – constituting the FINISH element.

Note that no EU NAVFOR asset was involved in this, but all was coordinated by EU NAVFOR's MSCHOA.

What I want to leave you with, however, is four key messages:

1) **Tools designed for piracy are still fit-for-purpose, but can now be transformed to cover other activities**
2) **You need to share information to build up your Maritime Domain Awareness (MDA).** Having the bigger picture allows action to be taken against illicit activity. If you only find out through your national system when a vessel enters your TTW, you're too late. But if your neighbor is able to give you the information when a vessel is still 300NM out, you have time to prepare and coordinate
3) **Information exchange is a two-way street**. Not because information is power, but because there needs to be utility in sharing information, as there is a cost (time, effort) in doing so. You cannot expect to receive information, but not give it – that's not how a partnership works. The only reasons shipping industry give us the information, is because we a) provide a guaranteed response when they are in distress, b) we give them information that informs their decision making, and c) they know we handle their confidential information with great care.
4) **You have to respond**. Even after 10 years, the partnership is tested every day. The moment we fail to respond two or three times in a row to a piracy attack, we're doomed.