

# WHAT WE KNOW ABOUT PIRACY



one earth  
FUTURE



**STABLE SEAS**

*a program of One Earth Future*



**SAFESEAS**



# WHAT WE KNOW ABOUT PIRACY

Author:

| Lydelle Joubert

May 2020

<http://dx.doi.org/10.18289/OEF.2020.046>

Design and layout by Liz Allen, One Earth Future.

Cover Image: HMS Monmouth's Boarding Team Approach a Dhow in the Arabian Gulf. Photo: Will Haigh, Defence Images.

# FOREWORD

*What We Know About Piracy* is the outcome of a collaboration between the [SafeSeas Network](#), based at the Universities of Bristol (UK) and Copenhagen (Denmark) and the [Stable Seas programme](#) of the One Earth Future Foundation. The report provides a comprehensive overview of the data available on piracy, drawing on desk-based research conducted between June 2019 and March 2020. It is the first of three reports and will be followed by similar data overviews on smuggling at sea and on maritime environmental crimes.

The research forms part of the research project *Transnational Organised Crime at Sea: New Evidence for Better Responses*, funded by the UK [Economic and Social Research Council](#) (ESRC) as part of UK Research and Innovation's (UKRI) [Partnership for Conflict, Crime and Security Research](#) (PaCCS) (Award Number: ES/S008810/1). Additional funding for the work was provided by the One Earth Future Foundation. Further information on the project is available at [www.safeseas.net](http://www.safeseas.net).

The report was authored by Lydelle Joubert (Stable Seas). Input and comments on earlier drafts were provided by Dr Curits Bell (Stable Seas), Professor Tim Edmunds (SafeSeas/University of Bristol), Dr Scott Edwards (SafeSeas/University of Bristol), and Professor Christian Bueger (SafeSeas/University of Copenhagen).



# TABLE OF CONTENTS

<b>I. INTRODUCTION .....</b>	<b>01</b>
<b>II. WHO COLLECTS DATA ON MARITIME PIRACY AND ARMED ROBBERY AGAINST SHIPS? .....</b>	<b>03</b>
Organizations Collecting Piracy Data on a Global Level .....	03
Organizations With a Regional Focus.....	06
Other Entities Collecting and Analyzing Piracy Data.....	09
Summary.....	10
<b>III. INFORMATION FLOWS: WHO IS REPORTING INCIDENTS, AND WHAT DATA IS COLLECTED BY ORGANIZATIONS.....</b>	<b>12</b>
<b>IV. QUANTIFYING AND ANALYZING MARITIME PIRACY AND ARMED ROBBERY AGAINST SHIPS .....</b>	<b>19</b>
Vessel Names .....	19
Data Mining, Patterns of Life, and Predictive Piracy Models.....	20
<b>V. DIFFERENTIATION PROBLEMS, LIMITATIONS, AND BLIND SPOTS .....</b>	<b>23</b>
<b>VI. CONCLUSION .....</b>	<b>25</b>
<b>ENDNOTES .....</b>	<b>26</b>



## I. INTRODUCTION

Transnational organized crime at sea manifests in multiple forms of illicit activity. One such form of crime is maritime piracy and armed robbery of ships. Information on piracy has been systematically collected since the 1980s when the International Maritime Organization and the International Chamber of Commerce started to compile such data. With the increase in piracy incidents in different maritime regions since the 1990s, the number of actors collecting data and analyzing these incidents has grown substantially. Data and analysis are now available from piracy reporting centers, international and regional organizations, naval services, the shipping industry, and the maritime media, as well as a wider expert community.

This paper provides the first systematic overview of how data on piracy and armed robbery is collected and what different kinds of information on piracy are available. The paper addresses how different organizations define, categorize, quantify, and analyze piracy. What common themes and issues can we identify? Who collects data and how? How accessible is the data? Where do we lack data? What are the blind spots?

First, providing this overview is important in order to get a better understanding of what the gaps in the data on piracy are. Second, it also allows stakeholders to identify divergences in data analysis and to better understand the reasons there are potentially conflicting numbers

and trends. In addition, such an overview constitutes a first step towards better harmonizing data to inform responses to piracy and strengthening overall analytical capabilities for maritime security.

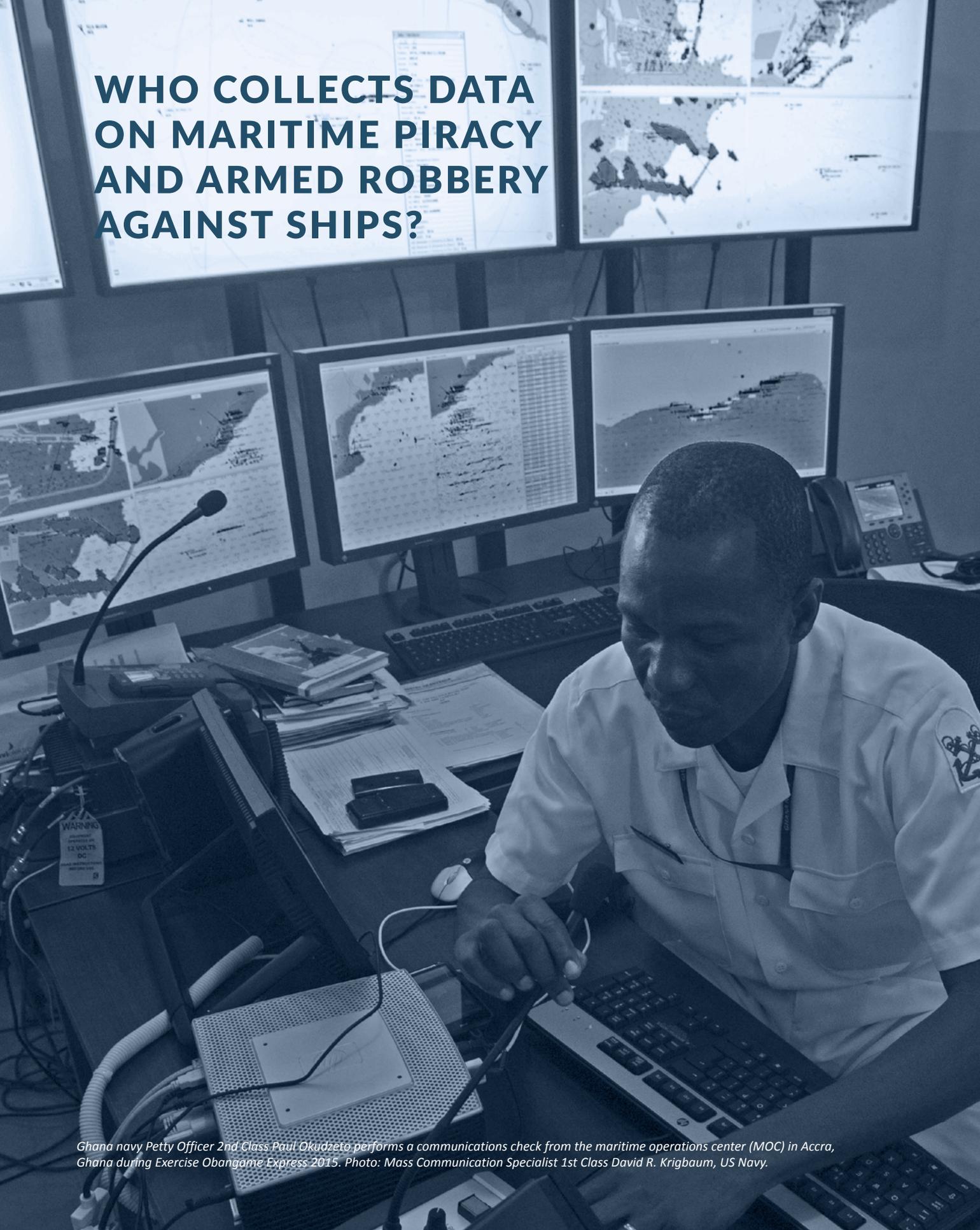
The paper starts with a systematic overview of the kinds of organizations that collect and analyze piracy data. It shows that the number of actors involved in collecting piracy data is quite substantial. The paper identifies six public entities collecting global piracy data and eight entities collecting region-specific data, as well as three additional non-governmental organizations and networks. In so doing, it documents the initial scale of data collection and analysis. In the next step, the paper investigates the flow of information and the kind of data points collected by these different organizations. Quite substantial divergences come to the fore. The next section evaluates the quality of the data to provide insights on the character, shape, and organizational structures of contemporary piracy. The concluding section then turns to the gaps in our understanding of piracy that the available data leaves.

*How is data on piracy and armed robbery collected? By whom? What kinds of information are available? How accessible is the data? What are the blind spots?*



*Sailors operate a twin-boom extensible crane during a joint U.S. and Philippine navy counter-piracy patrol in the Sulu and Celebes Seas. Photo: Mass Communication Specialist 3rd Class Deven Leigh Ellis, U.S. Navy.*

# WHO COLLECTS DATA ON MARITIME PIRACY AND ARMED ROBBERY AGAINST SHIPS?



*Ghana navy Petty Officer 2nd Class Paul Okudzeto performs a communications check from the maritime operations center (MOC) in Accra, Ghana during Exercise Obangame Express 2015. Photo: Mass Communication Specialist 1st Class David R. Krigbaum, US Navy.*

**GLOBALLY:**



The International Chamber of Commerce's International Maritime Bureau

🔒 ⚠️ **LIVE** **QT** **365**

International Maritime Organization

🔒 **LIVE** **31** **365**

The International Criminal Police Organization (INTERPOL)

🔒

US Office of Naval Intelligence (ONI)

🔒 **7**

The Maritime Information Cooperation and Awareness (MICA) Center

🔒 **365**

**CARIBBEAN**

Caribbean Community (CARICOM)

🔒

**Data Types & Accessibility**

- 🔒 Open-source database
- 🔒 Closed database
- ⚠️ Issues Alerts

**Frequency of Reports Published:**

- LIVE** Live updates
- 1** Daily
- 7** Weekly
- 31** Monthly
- QT** Quarterly
- 365** Annually

**GULF OF GUINEA**

Marine Domain Awareness for Trade-Gulf of Guinea (MDAT-GoG)

🔒 ⚠️ **7**

**GULF OF ADEN & HORN OF AFRICA**

Maritime Security Centre-Horn of Africa (MSCHOA)

🔒 ⚠️

European Union Naval Force Operation Atalanta (EU NAVFOR)

🔒

United Kingdom Maritime Trade Operations (UKMTO)

🔒 ⚠️ **7**

**GULF OF GUINEA TO SOUTHEAST ASIA**

Information Fusion Centre-Indian Ocean Region (IFC-IOR)

🔒 **31**

**WESTERN INDIAN OCEAN**

Regional Maritime Information Fusion Centre (CRFIM)

🔒 **7** **31** **365**

**ASIA**

The Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP)

🔒 ⚠️ **7** **31** **365**

Information Fusion Centre-Singapore

🔒 **1** **7** **31** **365**

## II. WHO COLLECTS DATA ON MARITIME PIRACY AND ARMED ROBBERY AGAINST SHIPS?

Multiple international and regional organizations collect and analyze data on piracy and armed robbery of ships. Reports by the International Maritime Bureau of the International Chamber of Commerce (IMB/ICC), by the International Maritime Organization (IMO), and by the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia Information Sharing Centre (ReCAAP-ISC) are the baseline for quantifiable data as they can be evaluated as the most complete and credible datasets for incidents of piracy and robbery of vessels. Incident data from the IMB and

ReCAAP-ISC are open-source and accessible to all users (except for a few fields which are security-sensitive). Users must register to use the IMO database, but regardless, data is available to the public.

This information, however, can still be incomplete since not all incidents will be reported to these entities. Below we provide a systematic overview of the data-collecting organizations.

### Organizations Collecting Piracy Data on a Global Level

Some international organizations collect data on incidents of piracy and armed robbery of ships, while others collect piracy-related court transcripts where additional information can be found on specific incidents, or data on pirate networks and individuals in these networks.

### *The International Chamber of Commerce's International Maritime Bureau*

The IMB was established in 1981 to act as a point of contact in the fight against all maritime crime, including maritime piracy and armed robbery of ships. The IMB Piracy Reporting Centre (PRC) was established in October 1992 in Kuala Lumpur, Malaysia. The PRC provides a live piracy report and online map of incidents of piracy and armed robbery.<sup>1</sup> In addition, it publishes quarterly and annual reports with detailed piracy and armed robbery statistics that can be downloaded from its website. According to Cyrus Mody,<sup>2</sup> assistant director at the ICC's Commercial Crime Services, incidents are reported to the PRC in various ways, but today masters of ships will most often phone the company or the PRC when under attack. The call will be followed up with a written report. The IMB receives 90 percent of its incident reports via the company or company security officer. The IMB will notify appropriate response agencies such as coast guards, marine police, or maritime authorities and will broadcast daily piracy and armed robbery status reports to ships via the Inmarsat-C SafetyNET service. The other ten percent of piracy and armed robbery-related incidents are received via the coastal state, United Kingdom Maritime Trade Operations (UKMTO), VHF radio, Digital Selective Calling (DSC), or other reporting agencies. Authorities will often contact the IMB to confirm whether it has additional information. All incidents in its database are verified with the company. In the case of a kidnapping or hijacking, the IMB will keep in touch with the owners until the crew or vessel is released. Coastal authorities will also let the IMB know of developments such as an arrest of pirates or robbers, although this is less likely to happen if the case drags on. The IMB will also share information with the IMO and other relevant reporting organizations.

The IMB does not differentiate between piracy (international waters) and armed robbery (territorial waters) as it is there to give ships' masters and owners a platform to make informed decisions about piracy and armed robbery in any given location. The risk to vessels will be the same whether an incident took place in international or territorial waters. The response by reacting authorities to the incident might, however, differ. IMB data was never intended to be a policy tool.

The IMB differentiates between actual and attempted attacks. Actual attacks are classified as "boarded" or "hijacked" and attempted attacks as "fired upon" or "attempted." The IMB quantifies the total attacks by country, ship status during attack, types of arms used in attacks, violence to crew, types of vessels attacked, flag state of ships, nationalities of crew, countries where victim ships are managed, and time of incident.

To address underreporting in the Gulf of Guinea, the IMB and Oceans Beyond Piracy conceived the "Community of Reporting," allowing all agencies and commercial operators to share incidents with the IMB in confidence. The IMB collates these incidents under levels I to III to show the percentage of underreporting. In the 2018 report, the recorded level of underreporting in the Gulf of Guinea was 48 percent.<sup>3</sup>

### *International Maritime Organization*

The IMO started to collect incident data in the 1980s. Since the 1990s, these reports have been collected in a dedicated digital database, the Global Integrated Shipping Information System (GISIS). Incidents of piracy and armed robbery of ships received from IMO member states and reporting international and regional organizations are incorporated in the IMO's GISIS.<sup>4</sup> GISIS also includes a database on ship and company details of the world's fleet of ships, as well as information on contact points of rescue coordination centers (RCCs) and Ship Security Alert Systems (SSAS); both systems are of value in analyzing piracy incidents. Access to GISIS is open-source but subject to registration. The plus point of the piracy database is that names of ships are published, which is of value when analyzing data, and also makes double reporting of incidents less likely. The database contains incidents since 1994. A downloadable Excel spreadsheet or report can be created from database searches. Locations of incidents, in terms of international or territorial waters or port area, status of ship when attacked, and number of people involved can be found in the Excel spreadsheet. The data report includes latitude and longitude of incidents since 2007, but excludes location and coastal state of incidents, which can be found and added from the GISIS database. Incidents can also be viewed on an online map.



*A map inside the IMB's Piracy Reporting Centre highlights piracy and armed robbery incidents. Photo: Jonas Gratzler.*

The IMO produces monthly incident reports and annual reports analyzing trends by region.<sup>5</sup> The IMO classifies any act of piracy (international waters) separately from armed robbery against ships (territorial waters). For the IMO, as the United Nations' regulatory body responsible for adopting new conventions and regulations to cater to the changing maritime security environment, the location of an incident in terms of international or territorial waters has different legal implications, and different conventions and regulations apply to different jurisdictions.

### *The International Criminal Police Organization (INTERPOL)*

In 2005 INTERPOL established Project BADA ("pirate" in Korean) targeting criminals involved in maritime piracy and acts of armed robbery of ships. The aim of the project is to bridge the gap between military interdiction and the prosecution of pirates. Information on individuals implicated in acts of maritime piracy and robbery of vessels is captured in INTERPOL's global databases. Piracy incidents, ransom payments, fingerprints, DNA profiles, telephone numbers, email addresses, locations, and financial information<sup>6</sup> from the 36 contributing countries are also included in the database.<sup>7</sup> Currently the database stores more than 4,000 records.<sup>8</sup> The digital album contains photos of more than 300 suspected

pirates. These photos can help identify suspects during debriefings with released hostages. The Stolen Vessels database is used to trace stolen vessels and engines. This information, however, is only available to law enforcement officers of member countries and international partners. The INTERPOL Maritime Piracy Task Force provides direct training to improve and analyze data. INTERPOL also investigates financial transactions and establishes links between piracy and other crimes, such as money laundering or terrorism.

### *United Nations Office on Drugs and Crime*

The United Nations Office on Drugs and Crime (UNODC) has been particularly active in building capacity for criminal justice mechanisms for the prosecution of suspected pirates once naval forces intercept and arrest them. As part of this work it collects data on piracy available from the criminal justice sector. Often datasets reveal more about failed attacks than actual attacks, at least in the short term. This is especially true of hijackings and long-term kidnappings where crewmembers are kept for many months and details only become available at the conclusion of the ordeal. During piracy trials, additional information is revealed about incidents, including a pirate group's modus operandi, the identities of criminals involved, and details regarding boarding,

weapons used, and circumstances contributing to the success of the attacks. The Sharing Electronic Resources and Laws on Crime (SHERLOC) portal is an initiative to facilitate the dissemination of information with regard to the implementation of the UN Convention against Transnational Organized Crime and its three protocols (the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children; the Protocol against the Smuggling of Migrants by Land, Sea and Air; and the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition). SHERLOC provides information on laws, jurisprudence, policies, and bibliographic abstracts with the aim of regulating the collection and use of electronic evidence in legal proceedings. All the resources displayed in this section can also be accessed directly within their respective databases from SHERLOC's front page.<sup>9</sup> Currently, 63 piracy cases can be found in the system, but case studies are mostly related to Somalian piracy, with limited cases from Mauritius, the US, the Netherlands, Kenya, and the Seychelles.

### *US Office of Naval Intelligence*

The US Office of Naval Intelligence (ONI) updates a weekly *Worldwide Threat to Shipping Report* that includes piracy and armed robbery incidents. The information in the report is mostly drawn from open-source information on incidents from international and regional organizations as well as media sources. In the report, the date and place of the incident, the name of the vessel, and the latitude and longitude and details of the incident are given. The locations of the incidents are also indicated on a map. A weekly piracy infographic can be found on the website. Incidents are classified in terms of kidnappings, hijackings, combined hijacking/kidnappings, boardings, and attacks/attempted boardings.<sup>10</sup> Archived reports dating from 1999 can be found in the Anti-Shipping Activity Messages (ASAM) database in the Homeland Security Digital Library.<sup>11</sup>

### *The Maritime Information Cooperation and Awareness Centre*

The Maritime Information Cooperation and Awareness (MICA) Center, based in Brest, France, was launched in June 2016. The center is run by the French navy and navies of partner countries and provides ships and their owners with risk assessments and alerts related to

maritime security. MICA published its first annual report on worldwide maritime piracy and robbery in early 2020, covering 2019 incidents. Incidents are classified as hijackings, attacks, boardings, and robberies. The MICA report distinguishes between piracy and armed robbery in its data. Hijackings and kidnapping incidents are combined in MICA's piracy statistics. This is because several of these events have been difficult to distinguish between and classify in recent years. However, combining the categories can be confusing. The country-by-country analysis in the report, consisting of a short overview and a graphic of incidents since 2008 in each country, is useful. The graphic indicates the normal trend for a country, and spikes in attacks can be clearly observed. The center has a very broad definition of piracy, including hijackings of vessels by migrants<sup>12</sup> and attacks on oil platforms. Although a list of piracy and armed robbery incidents is provided in the report, ships are not identified by name, nor are the reporting authorities or sources of information indicated, which makes it impossible to verify some incidents.

## **Organizations With a Regional Focus**

Masters of ships will often report incidents of piracy and armed robbery to regional organizations where incidents occur or to organizations associated with their flag states. These organizations will share information, confirm incidents, classify incidents, analyze data, and create reports to support masters of ships in risk assessments and to create maritime situational awareness in the areas they transit. Advice will also often be given.

### *The Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP)*

ReCAAP was established in November 2006, and was the first regional agreement to further cooperation against piracy and armed robbery against ships in Asia. Contracting parties to ReCAAP include North, Southeast, and South Asian countries as well as Norway, the Netherlands, Denmark, the United Kingdom, Australia, and the United States. The Information Sharing Centre's (ISC) role and activities support information sharing, capacity building, and cooperative arrangements between members by hosting workshops and meetings, among other activities.

The primary source for ReCAAP is its ISC's Information Network System (IFN). The ReCAAP Focal Points are located in member countries at either the department of shipping, marine police, coast guard, navy, maritime authority, or in some cases, the maritime rescue coordination centers (MRCCs).<sup>13</sup> ReCAAP-ISC incorporates incidents from the ReCAAP Focal Points and also receives and incorporates information from the IMO, Information Fusion Centres in Singapore and India (Indian Ocean Region), Malaysian and Indonesian authorities, ship owners, ship operators, ship agents, and commercial companies such as shipping companies as well as other publicly available sources such as media sources.<sup>14</sup> These sources are indicated in its reports. Ship owners, ship operators and shipping companies can report piracy and armed robbery incidents to the ReCAAP ISC using its online form.<sup>15</sup>

Piracy and armed robbery alerts; weekly, monthly, and annual reports on piracy and armed robbery of vessels in Asia; and piracy guidance-related reference documents for Asia, such as the Regional Guide to Counter Piracy and Armed Robbery Against Ships in Asia, are all available on the ReCAAP website.<sup>16</sup> So is an interactive map portal.<sup>17</sup> The ReCAAP ISC distinguishes between piracy and armed robbery incidents. However, because of a sensitivity among littoral states around territorial sovereignty with regard to possible foreign navy involvement in maritime security operations in their territorial waters, some incidents in the eastern approaches to the Straits of Malacca and Singapore are not classified as piracy, the fact that they took place in international waters notwithstanding. ReCAAP evaluates the significance of each piracy or armed robbery incident according to the level of violence and the economic loss incurred as determined by the type of property taken. The level of violence is determined by the type of weapon used, the treatment of crew (from theft to kidnapping and killing of crew), and the number of perpetrators involved. Incidents are classified from CAT 1 to CAT 4 and attempted attacks, with CAT 1 the more serious. Similarly, and as with the IMB, ReCAAP also quantifies the total attacks by status of ship during attack, types of arms used in attacks, violence to crew, types of vessels attacked, and time of incident. The number of perpetrators and type of losses are also reported. In recent years ReCAAP has enhanced its analysis in reports with the help of data analytics where it provides insight into trends and detailed analyses of

incidents based on data accumulated over more than a decade.<sup>18</sup> ReCAAP verifies all the incidents with its Focal Points, who could be in the flag state of the ship, the coastal state where the incident occurred, regional authorities, and so on.<sup>19</sup>

### *Information Fusion Centre–Singapore*

The Information Fusion Centre (IFC)<sup>20</sup>–Singapore, hosted by the Republic of Singapore Navy, is one of three IFCs, the others being in India and Madagascar. The IFC–Singapore was established on 27 April 2009. Nineteen international liaison officers from 18 countries are currently represented at the center. The center is also linked with 97 agencies in 41 countries. The IFC collects and fuses data on all maritime security-related incidents in the Asian region. This includes piracy.

The IFC distributes a monthly maritime security incident map, an annual report, weekly reports, daily reports, and spot commentaries for the Southeast Asia region. Piracy and armed robbery of ships is one of the IFC's crime categories. The center differentiates between theft, robbery, and piracy at sea; and have kidnap-hijack/attack, sea robbery, sea theft, attempted action, and suspicious approaches as subcategories. The IFC relies on open-source data including media reports and information from the Focal Points that was reported to local or flag-state countries. Incidents by type of vessel, hotspots, and level of violence are analyzed in the annual report. The difference between sea robbery (armed robbery) and sea theft (nonviolent theft) is not immediately evident in the reports but both are defined in annual reports.

### *Regional Maritime Information Fusion Centre*

In 2013 the Regional Maritime Security Programme (MASE Programme) financed by the European Union and coordinated by the Indian Ocean Commission (IOC) was established in the eastern and southern Africa and Indian Ocean (ESA-IO) region. In April 2018, five states from the ESA-IO region, Djibouti, Madagascar, Mauritius, and the Union of Comoros and Seychelles, signed the Agreement for the Setting up of a Regional Maritime Information Exchange and Sharing Mechanism in the Western Indian Ocean at the Ministerial Conference on Maritime Safety and Security held in Mauritius. The objective of the Regional Maritime Information Fusion Centre (CRFIM) is to improve regional maritime situational awareness, to

monitor maritime activities and crimes, and to promote maritime information exchange between the center and national, regional, and international centers.<sup>21</sup>

CRFIM reports focus on incidents of piracy and armed robbery in the ESA-IO region, which it categorizes under “violence at sea.” CRFIM has weekly activity reports, and monthly and annual reports which include other maritime crimes such as illegal, unreported, and unregulated (IUU) fishing, the smuggling of contraband at sea, human trafficking at sea, and other types of smuggling activities. Information in the reports is obtained from internal and external sources such as operation centers and maritime stakeholders.

According to CRFIM, coastal states have no problems sharing safety information, but when it comes to armed robbery in their coastal waters, countries see it as an internal problem. Countries are not keen to expose their internal security problems. CRFIM aims to improve the situation by having country liaison officers from individual countries placed at the center. The center also has contacts in harbors, but the information received is not always firsthand information.<sup>22</sup>

### *European Union Naval Force Operation Atalanta*

The EU launched the European Union Naval Force (EU NAVFOR) Operation Atalanta in December 2008. In 2018 the mission’s mandate was extended to December 2020. EU NAVFOR’s objective is to deter and disrupt acts of piracy and armed robbery on the high seas in the area of operations covering the southern Red Sea, the Gulf of Aden, and a large part of the Indian Ocean, including Somalia, Seychelles, Mauritius, and Comoros.

Piracy incidents in the EU NAVFOR area of operations are published in short posts under the “News” heading on their website.<sup>23</sup> Archived incident information can be found on the website as well.

### *Maritime Security Centre–Horn of Africa (MSCHOA)*

MSCHOA, located in Brest, France, is an initiative established by EU NAVFOR and is the “maritime industry control centre” for the EU’s Operation Atalanta.<sup>24</sup> Security concerns limit access to the secure part of the website to registered users from shipping companies. Basic piracy statistics as well as news can be found on the

MSCHOA website.<sup>25</sup> Threat assessments and alerts for the High Risk Area and the Western Indian Ocean, and global piracy guidance reference documents such as Best Management Practices (BMP5), are also located on the website.

### *United Kingdom Maritime Trade Operations*

United Kingdom Maritime Trade Operations (UKMTO) is an entity of the Royal Navy and provides a point of contact and information link between security forces and international maritime trade organizations and actors. UKMTO receives information from several organizations, operational centers, and port authorities within the Indian Ocean region.<sup>26</sup>

Although it seems that UKMTO receives very little information in its incident format, it receives additional information in reports prior to vessels entering the high-risk area off Somalia. UKMTO reports are intended to create maritime situational awareness for mariners operating in the Indian Ocean and its High Risk Area (HRA) and to warn masters about possible risks. UKMTO does not verify security events. Advisory notices are not descriptive and do not distinguish between piracy and conflict-related events. Weekly reports have been provided since 2017 and are available on its website. These reports provide additional information and indicate if an incident is classified as piracy. Vessels and type of vessel are not always identified.

### *Information Fusion Centre–Indian Ocean Region (IFC-IOR)*

IFC-IOR is a center operated by the government of India. It was launched in December 2018 in Gurugram, India, and is closely associated with the Information Management and Analysis Centre (IMAC) jointly run by the Indian Navy and Indian Coast Guard. Their aim is to collate, fuse, and disseminate intelligence on maritime threats from the Gulf of Guinea to Southeast Asia. Piracy and Sea Robbery is one of the six broad crime categories. Others are Maritime Terrorism, Contraband Smuggling, Irregular Human Migration, IUU Fishing, and Maritime Incidents.<sup>27</sup> Incidents are collected in four sectors: Sector A-Gulf of Guinea, Sector B-Gulf of Aden and the Arabian Sea, Sector C-Bay of Bengal, and Sector D-South East Asia. Monthly maritime security reports are available on the IFC-IOR website.<sup>28</sup>

IFC-IOR signed information exchange agreements with 22 countries and aims to base 40 liaison officers from partner countries at the center. Only a few countries, such as France, have so far placed officers, but the center expects to have four to five officers placed by mid-2020.<sup>29</sup> The center differentiates between piracy and armed robbery and has hijacking, kidnapping, sea robbery (armed), sea theft (nonviolent), attempted boarding, and suspicious approach as subcategories. Its main data source is ReCAAP, as data is validated by the Focal Points in ReCAAP-contracting countries. The center has some concerns about insurance fraud in datasets of other international organizations as the data is not always validated by the flag states. IFC-IOR currently has no capability for verifying incidents themselves, but does expect that this will improve with the placement of more liaison officers at the center. The placement of liaison officers is also expected to improve trust between countries, which is hoped will make them more likely to share information with each other. Incidents in the internal waters of coastal states, such as kidnappings in the Bangladeshi Sundarbans, which are not reported in official statistics, are some areas of concern for the center.

### *Marine Domain Awareness for Trade–Gulf of Guinea (MDAT-GoG)*

MDAT-GoG<sup>30</sup> is a cooperation center in support of the Yaoundé Process that is operated by the Royal Navy (UKMTO) based in Portsmouth, UK, and the French Navy (MICA-Center) centered in Brest, France. It started operations in June 2016. MDAT-GoG issues a weekly piracy and armed robbery report based on information sent from vessels using the Voluntary Reporting Scheme. It also publishes a live map of incidents on its website. Incidents can be filtered to view different event types and period filters for 10, 30, 90, and 365 days. The aim of the reports is to provide maritime situational awareness for mariners operating in the Gulf of Guinea, and incidents are not verified. Incidents are classified as hijack-kidnapping, boarding-boarding attempt, attack, robbery-sea theft, suspicious approach, and sighting-irregular activity. Names of vessels are not included, and in some cases the type of vessel attacked is also excluded.

### *Caribbean Community (CARICOM)*

In Latin America and the Caribbean, piracy and armed robbery are underreported as they do not currently

pose a significant risk to commercial shipping. Regional organizations and governments also see these as an internal problem, as most incidents in this region take place in the territorial waters of countries. The Caribbean islands are located in a sea area of 2.75 million square kilometers, and capacity is also lacking in several countries. The focus of the Caribbean Community (CARICOM) Implementation Agency for Crime and Security (IMPACS) is more on other security concerns, such as terrorism and trafficking in drugs, arms, and humans, than piracy and armed robbery of ships. Armed robbery of vessels is addressed as part of a wider security concern.<sup>31</sup>

## Other Entities Collecting and Analyzing Piracy Data

Several other organizations and NGOs, maritime risk companies, and insurance associations are keeping datasets for specific purposes. They might be interested in the human cost of piracy, or in specific maritime sectors such as yachts/cruisers or commercial vessels. These interests will dictate what data is collected and how it is classified.

### *Stable Seas*

Stable Seas is a program of One Earth Future, and publishes an annual *State of Maritime Piracy Report*. The report aims to quantify the human cost of piracy and to identify and analyze trends in maritime piracy and robbery of vessels worldwide to create a better understanding of the global piracy problem and the ways in which it affects maritime stakeholders. The data sources used in compiling the report are the main maritime piracy reporting organizations such as the IMB, the IMO, ReCAAP-ISC, insurance companies, maritime security companies, shipping companies, and the media. The report not only includes attacks against commercial vessels, but also attacks on fishing vessels. Incidents are classified by location, and delineated as international, territorial, or internal waters. Incident types are classified as hijacking, kidnapping, armed robbery, robbery, and failed attacks. Incidents themselves are not listed in the report.<sup>32</sup> The report indicates the status of the ship during attack, types of vessels attacked, types of arms used in attacks, type of violence against crew, and nationalities of the crew.

### *Maritime Risk and Security Companies and War Risk Insurance Associations*

Several maritime risk and security companies compile their own piracy reports as part of the risk assessments they do for their clients. Some companies, such as Maritime Asset Security and Training (MAST),<sup>33</sup> will publish free online security and risk reports, while for others, risk assessments will be a payable service available to members or by subscription. Most security companies only collect information in their areas of operation and only have interest in attacks on commercial vessels.<sup>34</sup> This is why incidents in South and Central America and the Caribbean are not often included in reports. These companies are often not interested in incidents on non-commercial vessels as attacks on these vessels have a different risk profile than those on commercial vessels and often have a low impact on commercial traffic. Trading or sharing of information between security companies, shipping companies, and insurance companies is a common practice. Companies also make use of additional sources of information such as port agents or employees embedded in their regions of operation, which will give them access to the often-unreported incidents. As some of these companies are involved in hostage negotiations, they will often have a better understanding of the areas of operation of these pirate groups. Insured vessels will be more likely to report incidents. As War Risk Insurance associations insure vessels against war-related perils, they will conduct a survey or investigation on a vessel post-piracy incident<sup>35</sup> where additional details of the incident will come to light.

### *Caribbean Safety and Security Net and Noonsite*

The Caribbean Safety and Security Net<sup>36</sup> (CSSN) and Noonsite<sup>37</sup> are two volunteer-based organizations reporting piracy and armed robbery on yachts in the Caribbean. CSSN also provides basic precaution advice and lessons learned as a result of their analysis of incidents on cruisers. Information is based on self-reporting of incidents by owners of yachts involved and information from other parties with knowledge of incidents. Reports can be made via an online reporting form. They collect basic information such as time of attack, date, location, type of incident, and details of incident. CSSN confirms and clarifies incidents by email with reporting individuals but will also follow up on more serious incidents where

possible with the police and other authorities. In this case, an update will be published. CSSN and Noonsite share information between the two sites. Reports are classified as firsthand reports when incidents are reported by owners of vessels involved; secondhand and thirdhand reports indicate the source of the report in terms of potential reliability. It is recommended to only add second- and thirdhand reports to research datasets if the incidents can be verified by independent sources. Names of vessels are not published. CSSN also issues annual reports. In the reports, they differentiate between violent and nonviolent crimes, piracy, robbery, and suspicious activity. A wide range of subcategories are used. These are assault, assault/death, piracy, attempted piracy, robbery, suspicious activity, violent crime, burglary, attempted burglary, theft, attempted theft, vandalism, and nonviolent crime. A 10-year database is available online. The reliability of the reports is not indicated in the database.

### **Summary**

There is an underlying commonality and understanding in classification of data and themes in data by different organizations. Data from different reporting organizations may seem to validate incidents, but the information contained in individual incidents reported by the IMO, IMB, and ReCAAP-ISC is often very similar as they trace back to one source—the victim ship’s report to reporting authorities or the rescue coordination center of the coastal state. This also indicates that there is a high level of information-sharing between organizations.

Some incidents are investigated by authorities of the coastal state and the ship’s insurance companies. Press releases by ship companies or governments, EU NAVFOR, and media reports also often confirm incidents. Some information will be added to reports by international organizations, such as arrest information received from coastal authorities, as well as release dates of hostages and ship security advice.

# INFORMATION FLOWS: WHO IS REPORTING INCIDENTS, AND WHAT DATA IS COLLECTED BY ORGANIZATIONS



*Two container ships pass each other in a channel. Photo: Louis Vest.*

### III. INFORMATION FLOWS: WHO IS REPORTING INCIDENTS, AND WHAT DATA IS COLLECTED BY ORGANIZATIONS

As the above overview documents, different organizations collect data to serve different purposes. Some international organizations will collect data to support policymakers in decision-making while others collect data to create a better understanding of the maritime domain or in support of risk assessment to serve clients. The purpose of collection will determine what data is collected and what is dismissed. It will also determine the underlying themes of the data. For an international organization involved in policy recommendations, and coastal authorities responsible for security and rule of law in their territorial waters, whether the location of a maritime incident is in international or territorial waters is an issue of great importance. For ship insurance companies or ship security providers, it is of little

consequence, as the risk to commercial vessels will be the same whether the incident occurred in territorial or international waters.

Typologies are used to create a better understanding of the nature of piracy and robbery against vessels. All reports use the same standard fields such as flag, gross tonnage, type of ship, time of incident, location of incident, status of ship during the attack, and weapons used by attackers. The differences are in the classification of incidents by type of attack and level of violence during the attack. These classifications are usually defined in the different reports.

Interviewing hostages after their release not only assists in collecting evidence to prosecute pirates but also supplies additional intelligence regarding method of attack, location of captivity, and pirate identities, as well as the identities of other hostages held at the same location or nearby. INTERPOL, insurance companies, and large shipping companies interview hostages after release. Several other sources and data-gathering techniques are used by organizations to create a better understanding of piracy and armed robbery of vessels. The table below provides an overview of the techniques used to analyze data.

TABLE 1: DATA SOURCES ON PIRACY AND ARMED ROBBERY OF SHIPS

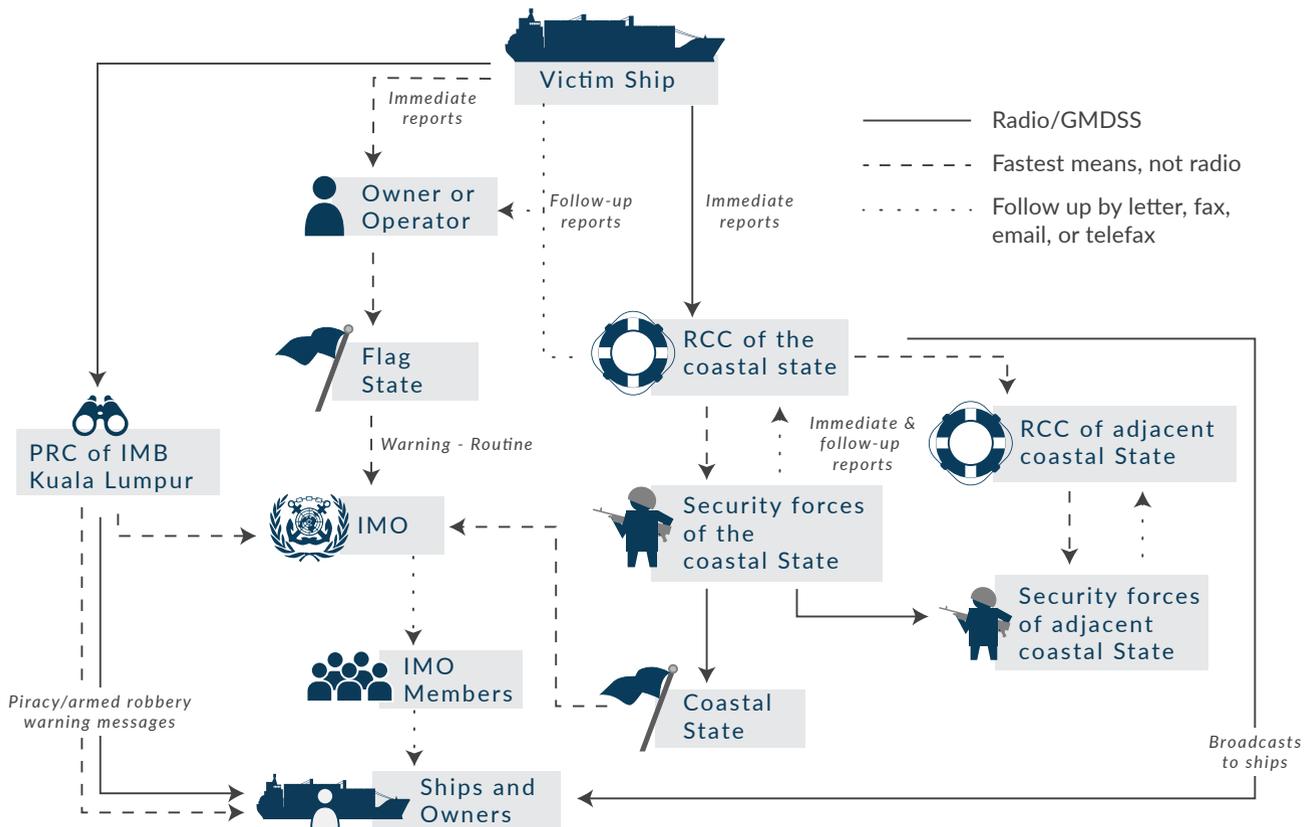
 <b>HUMAN</b>	Interview pirates or robbers captured/ arrested	 <b>GEOSPATIAL</b>	Data analysis
	Interview hostages or victims of piracy		AIS data analysis
	Patrols		Media reports
	Communication with fishers and locals		Press releases by shipping companies or European Union Naval Forces (EU NAVFOR)
 <b>SIGNALS</b>	Automatic Identification System (AIS)	 <b>OPEN SOURCE</b>	Legal transcripts of piracy court cases
	VHF radio		Research publications
	CCTV		Shipping data and registers
	Ship Security Alert System (SSAS)		Bibliographic data on pirates, such as fingerprints, photos, and DNA profiles
	Long Range Identification & Tracking (LRIT)		Crime scene evidence
Digital Selective Calling (DSC) system and Inmarsat-C	 <b>FINANCIAL</b>	Tracking ransom payments	
Voyage data recorder (VDR) data			

The International Maritime Organization (IMO) recommends specific procedures for reporting piracy and armed robbery incidents in its “Recommendations to Governments for preventing and suppressing piracy and armed robbery against ships” document [MSC.1-Circ.1333-Rev.1](#). It is recommended that the rescue coordination center (RCC) in the coastal state which is the first point for reporting should forward all reports of piracy and armed robbery to the IMO, International Maritime Bureau (IMB), and the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP). The recommended procedures for reporting are highlighted in the following flow diagrams.

In principle, all attacks, or threats of attack, should immediately be reported to the closest RCC or coastal radio station to alert the coastal state. The initial report should be followed up by a more detailed written report. On receipt of a radio report of an attack, the RCC must inform the local security authorities to assist the vessel under attack, alert other ships in the area, and inform adjacent RCCs.<sup>38</sup>

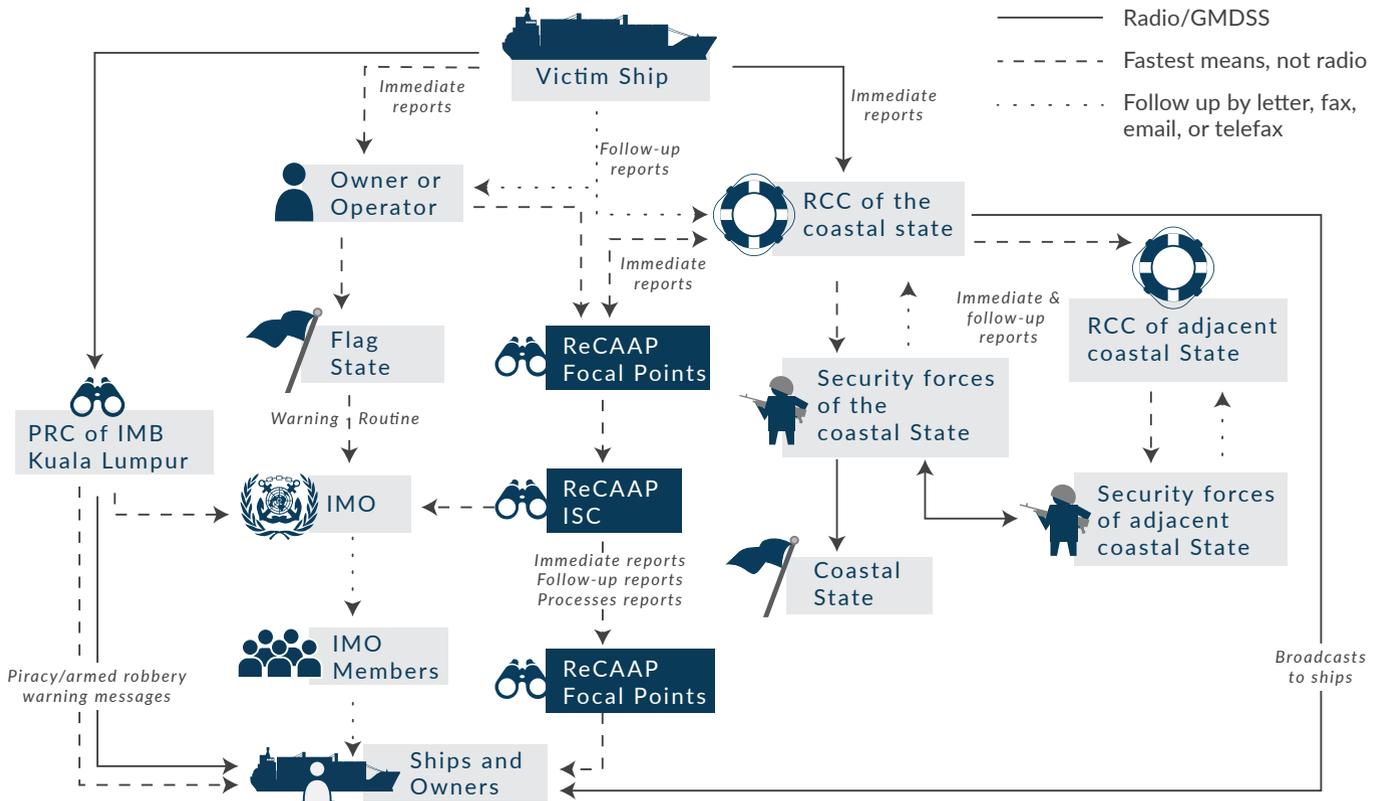
Information is first collected when the victim vessel sends a distress call on VHF radio channel 16 (the internationally recognized band for distress) to the RCC of the coastal state. The ship’s name and call sign, IMO number, Inmarsat IDs (plus ocean region code) and Maritime Mobile Service Identity (MMSI), position (and time of position UTC), latitude and longitude, course, speed, and nature of the event will be included in the message.

FIGURE 1: FLOW DIAGRAM FOR REPORTING INCIDENTS IN COASTAL WATERS



Adapted from: IMO, MSC.1-CIRC.1333-REV.1 (E).

FIGURE 2: FLOW DIAGRAM FOR REPORTING INCIDENTS IN ASIA



Adapted from: IMO, MSC.1-CIRC.1333-REV.1 (E).

In the follow-up report, the following information will be included: date; time; course; speed; position; was the vessel sailing, at anchor, or at berth; method of attack; description/number of suspect craft; number and brief description of pirates/robbers; kind of weapons the pirates/robbers carried; any other relevant information (e.g., language spoken); injuries to crew and passengers; damage to vessel; property stolen; action taken by the master and crew; whether the incident was reported to the coastal authority, and if so to which one; action taken by the coastal state; description of pirate craft; assistance needed; and preferred communications (HF/MF/VHF/Inmarsat ID). These data will also be the fields for later reporting to the IMO, IMB, and ReCAAP.

A distress message can also be sent via the DSC system and Inmarsat-C. Under the Global Maritime Distress and Safety System (GMDSS), all passenger ships and ships

over 300 gross tons on international voyages are required to be equipped with satellite and terrestrial radio communication systems enabling the vessels to send and receive distress alerts and safety communications.<sup>39</sup>

In addition, the SSAS should be activated to transmit a security alert to a competent authority to indicate the vessel is under attack. It will usually have two covert activation points, one of which will be on the bridge.<sup>40</sup> SSAS will transmit the ship's identity and current position. It will be addressed to a shore station. The appropriate shore station is listed in the IMO's GISIS.

Incidents will be reported to the IMO, IMB, ReCAAP-ISC, UKMTO and MDAT-GoG via phone or email. Most of these international reporting organizations offer a 24-hour service for shipmasters to report piracy and armed robbery incidents.

In reality, ships will often not follow the recommended IMO reporting procedure to the letter. The sea is unpredictable, and in an emergency the master and crew will do what they deem most effective to get immediate assistance. Today, most commercial vessels will have satellite phones, and in the event of an attack or a potential attack the master or ship security officer will call the company or company security officer, IMB PRC, regional reporting centres, MDAT-GoG or UKMTO, which will inform all relevant international, regional and national maritime operational centres. The IMO incident report in GISIS includes fields to indicate if the incident was reported and to which coastal authority, and actions taken by international reporting agencies.

Table 2 lists the fields in the reports to the IMO, IMB, ReCAAP-ISC, UKMTO and MDAT-GoG. The specific classifications in the IMB report are used and may not

be the exact wording used in IMO, ReCAAP-ISC, UKMTO and MDAT-GoG reports in order to make comparison possible. Overall, there is a great deal of overlap in the fields different organizations use, which helps to create a common understanding of themes.

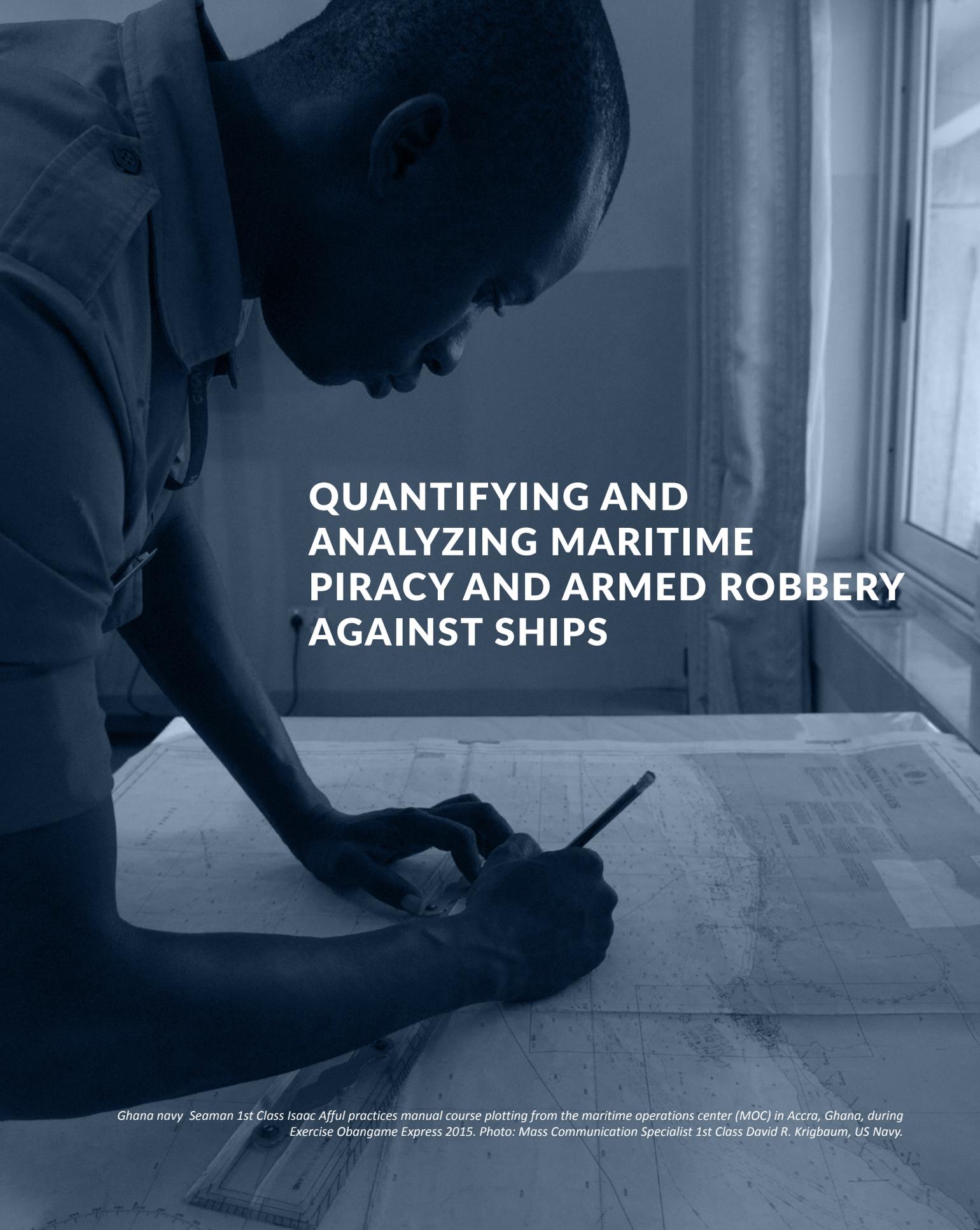
While piracy and armed robbery are reported to organizations responsible for assisting vessels under attack, or organizations that will alert vessels of a possible risk in the vicinity of an attack, these organizations are not the only ones collecting data. While some organizations will be interested in incident-related data, others will collect data on pirate groups and networks or gather information in support of prosecution of pirates. Collectively all these data will create domain awareness about piracy threats in a specific location. The next section addresses how piracy data can be used in analyses of trends and patterns.

TABLE 2: INFORMATION REPORTED TO INTERNATIONAL ORGANIZATIONS

	INFORMATION	IMB	IMO	RECAAP	UKMTO	MDAT-GOG
<b>PART A: VESSEL PARTICULARS/DETAILS</b>	Name of Ship	X	X	X	X	X
	IMO No.	X	X	X	X	X
	MMSI No.			X		
	IMMARSAT ID			X	X	
	Flag	X	X	X	X	
	Type of Ship	X	X	X		
	Call Sign			X		X
	Tonnages: GRT	X	X	X		
	NRT	X				
	DWT	X				
	Owners <i>(Address &amp; Contact Details)</i>	X		X		
	Managers <i>(Address &amp; Contact Details)</i>	X		X		
	Company Security Officer <i>(Name &amp; Contact Details)</i>				X	
	Last Port/ Next Port/ Time Arrival	X			X	
	Cargo Details <i>(Type/Quantity)</i>	X			X	

	INFORMATION	IMB	IMO	RECAAP	UKMTO	MDAT-GOG
<b>PART B: DETAILS OF INCIDENT</b>	Date & Time of Incident	X	X	X	X	X
	Position	X	X	X	X	X
	Nearest Landmark/Location	X	X	X		
	Port/Town/Anchorage Area	X	X			
	Country/ Nearest Country	X	X	X		
	Status ( <i>Berthed/ Anchored/ Steaming</i> )	X	X	X		
	Isps Level			X		
	Course				X	X
	Own Ship's Speed	X			X	X
	Ship's Freeboard During Attack	X			X	
	Weather During Attack ( <i>Rain/Fog/ Mist/Clear/Etc.</i> ); <i>Sea/ Swell Height</i> )	X				
	Weather During Attack: Wind ( <i>Speed &amp; Direction</i> )	X				
	Weather During Attack: Sea	X				
	Weather During Attack: Swell	X				
	Types Of Attack ( <i>Boarded/Fired Upon/ Attempted</i> )	X	X	X		X
	Consequences For Crew, Ship, & Cargo ( <i>Any crew injured/killed; items/ cash stolen</i> )	X	X	X		
	Nationalities Of Master & Crew	X			X	
Area Of The Ship Being Attacked	X	X				
<b>PART C: DETAILS OF RAIDING PARTY</b>	Number Of Pirates/Robbers	X	X	X		
	Dress/Physical Appearance	X	X	X		
	Language Spoken	X	X			
	Distinctive Details	X	X			
	Craft Used	X	X	X		X
	Closest Point Of Approach (CPA)	X	X			
	Method Of Approach	X	X			
	Duration Of Attack	X	X			
	Aggressive/ Violent	X	X			

	INFORMATION	IMB	IMO	RECAAP	UKMTO	MDAT-GOG
<b>PART D: DETAILS OF WEAPONS USED AND DAMAGE CAUSED</b>	Weapons Sighted <i>(Yes/No)</i>	X	X			
	Weapon Type	X	X	X		
	Weapons Used <i>(Yes/No)</i>	X	X	X		
	Damage Caused <i>(Yes/No)</i>	X	X	X		
	Details Of Damage <i>(Please Give as Much Information as Possible)</i>	X	X	X		
	Ladders Sighted <i>(Yes/No)</i>	X	X			
	Other Boarding Equipment Sighted <i>(Please Give Details)</i>	X	X			
<b>PART E: FURTHER DETAILS</b>	Action Taken by Master & Crew	X	X	X		
	Armed/Unarmed Security Team Embarked	X			X	
	Was Incident Reported to The Coastal Authority? If So, To Whom?	X	X	X		
	Action Taken by The Authorities	X	X	X		
	Anti-Piracy Measures Employed <i>(Please Specify)</i>	X	X	X		
	Source of Information			X		

A man in a military uniform is shown in profile, leaning over a table and plotting a course on a large map. He is holding a pen in his right hand and pointing with his left hand. The map is spread out on the table, and a ruler is visible in the foreground. The background shows a window with curtains. The entire image has a blue tint.

# QUANTIFYING AND ANALYZING MARITIME PIRACY AND ARMED ROBBERY AGAINST SHIPS

*Ghana navy Seaman 1st Class Isaac Afful practices manual course plotting from the maritime operations center (MOC) in Accra, Ghana, during Exercise Obangame Express 2015. Photo: Mass Communication Specialist 1st Class David R. Krigbaum, US Navy.*

## IV. QUANTIFYING AND ANALYZING MARITIME PIRACY AND ARMED ROBBERY AGAINST SHIPS

Not all data fields can be quantifiable, but some fields could be useful in identifying patterns. Simply quantifying incidents is not enough; incidents should be analyzed in terms of how they influence and relate to other fields.

### Vessel Names

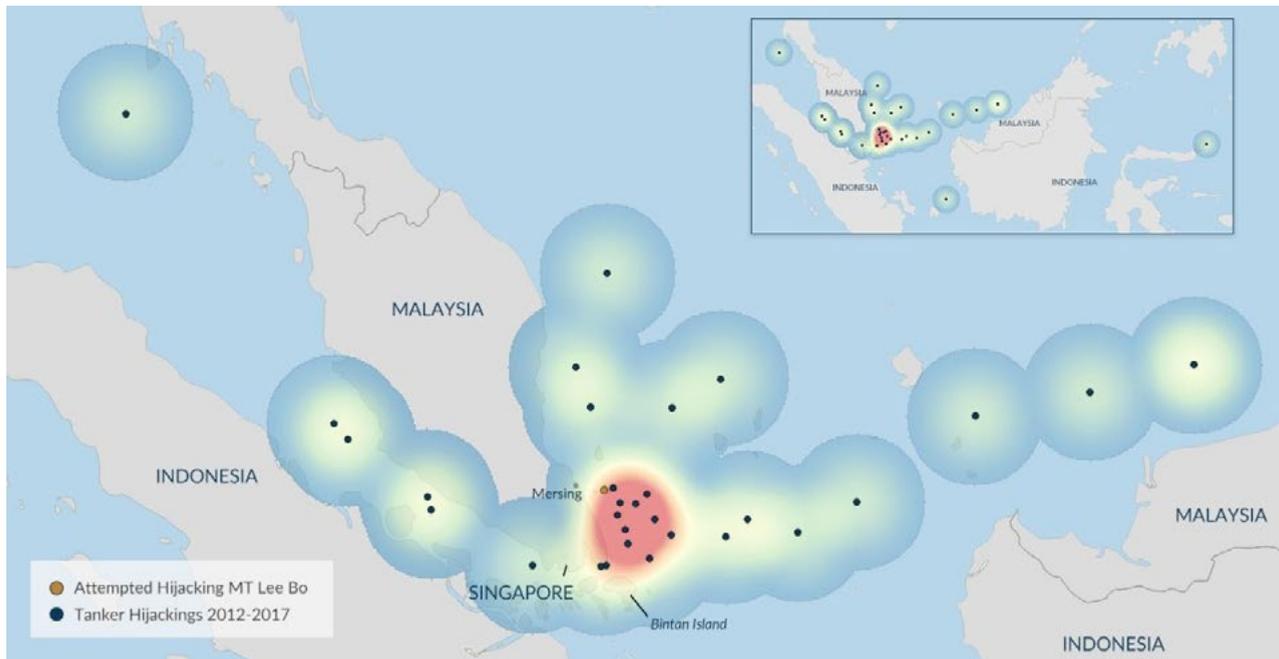
A great deal of information might be uncovered from the name of the vessel. The name of a ship is often important in identifying patterns. Repeat attacks on the same vessels are often reported. If the vessel is not identified by the reporting organization, it is not possible to know if an attack was reported on the same vessel previously. Repeat attacks are more common with certain types of vessels, such as tugboats. Tugboats towing barges often follow a schedule which makes them prone to

repeat attacks, and barges have a low freeboard which allows for easy boarding. Vessels involved in piracy and armed robbery incidents often report repeat attacks or suspicious approaches after initial attacks. Some vessels are more prone to repeat attacks as a result of their construction, which may make it easy to board, or due to predictable schedules, lack of security measures, fraud, or insider help, to list a few.

Shipping companies or owners occasionally give similar names to vessels, which can alert us to patterns. Between August 2013 and October 2013 attacks were reported on the tankers *Danai 3*, *Danai 4*, and *Danai 6*. By identifying the owners in the IMO GISIS system, two more tankers involved in attacks (*Oripin 2* and *Oripin 4*) were identified. Three of these attacks led to hijackings for product. All these attacks were at night, occurring between 20:00 and 22:30.

*Simply quantifying incidents is not enough; incidents should be analyzed in terms of how they influence and relate to other fields.*

FIGURE 1: PATTERN OF TANKER HIJACKINGS IN SOUTHEAST ASIA 2012 TO 2018  
A clear pattern is discernible.



Source: *Stable Seas*, State of Piracy Report 2018.



*EU NAVFOR Somalia Operation Atalanta flagship FS Siroco in cooperation with Japanese assets apprehended the crew of a dhow that was suspected to have been used as pirate mother-ship in 2014. Photo: European Union Naval Force.*

Not only was this company targeted five times, but patterns demonstrated that tankers from several companies were targeted repeatedly. Canter Marine of Singapore reported eight attacks between August 2013 and November 2015. This was clearly the same syndicate involved, and the pattern suggested that the attackers were able to make use of insiders for intelligence on the cargo and operational procedures. The geographical locations of several attacks also followed a pattern.

Insider collaboration in the hijackings was confirmed on 24 August 2014 when the captains of the Canter-owned *Moresby 9* and the MT *Victory Star* were caught red-handed by the Malaysian Maritime Enforcement Agency while transferring 50,000 liters of fuel off the *Moresby 9* to the MT *Victory Star* 12 nautical miles off Muka Head, Penang, Malaysia.<sup>41</sup>

*Vessel attributes, types of cargo carried, time of day, area of operations, and even sea states are all factors in predicting which vessels may be vulnerable to attack.*

## Data Mining, Patterns of Life, and Predictive Piracy Models

Certain vessel attributes (such as maximum speed capability, freeboard, construction, and schedule) as well as time of day and area of operations make a vessel more vulnerable to attack. In certain areas, certain ships are more likely to be targeted because of the cargo they carry. Sea state also affects the likelihood of success of an attack. It is difficult to board vessels in heavy seas as you have to move from one unstable platform to another. It is difficult to launch an attack when high wave heights and high wind speed are present.

Patterns of life and fishing vessel activity are used to determine what a typical pattern of a piracy operation will look like and whether there is a deviation from normal patterns. Analyses of these attributes are used to implement anti-piracy measures to protect vessels against attacks, such as those contained in Best Management Practices (BMP5 and BMP West Africa).

Naval forces also use such analysis to support command decisions. To address the challenge of covering a large area of operations with limited naval resources, for instance, analysts at the Combined Maritime Forces operating in

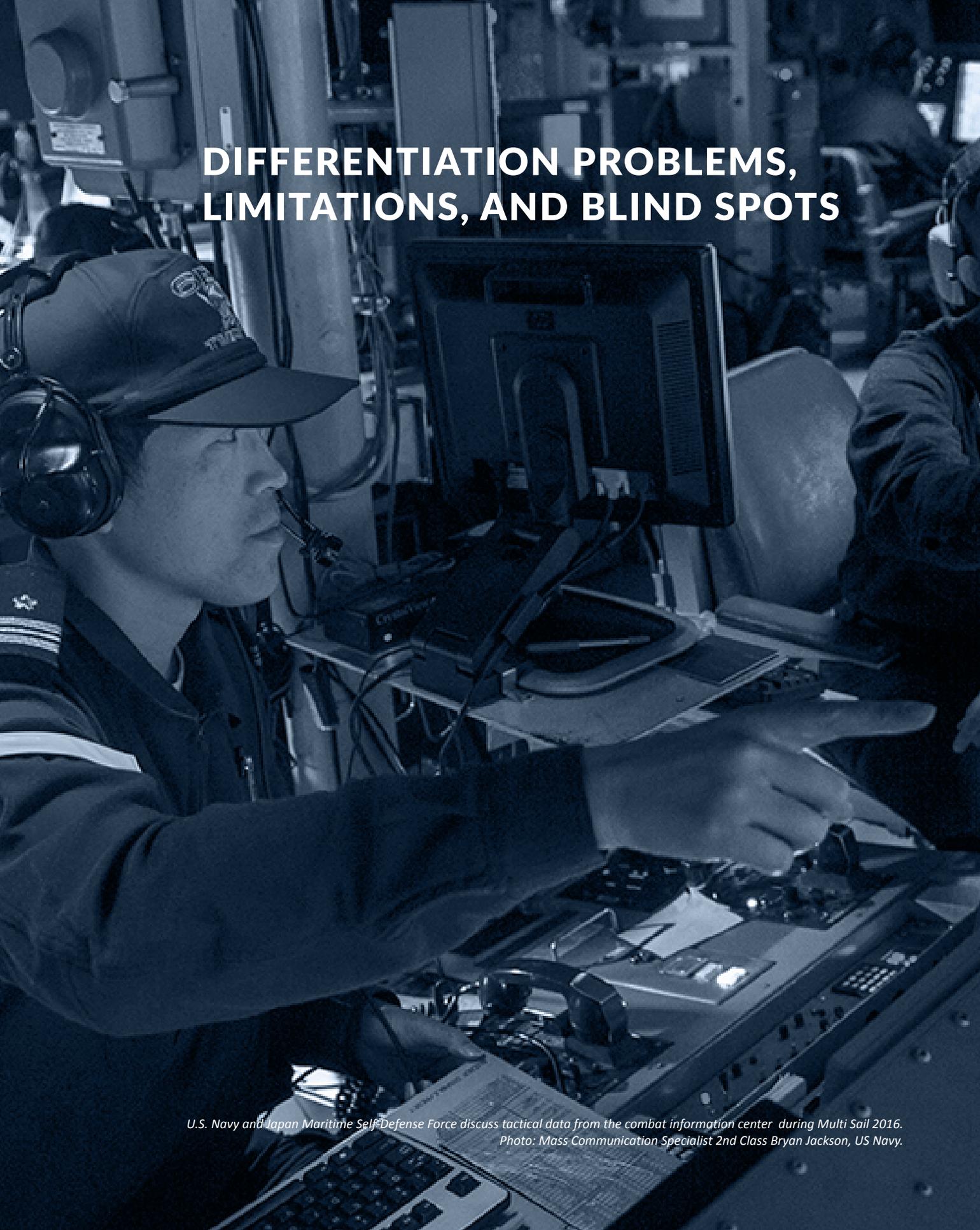
the Western Indian Ocean use spatial analysis of piracy attacks, predictive models to forecast piracy risk based on past attacks, maritime traffic patterns, and weather patterns to calculate the recommended patrol area size per asset to be able to intervene in a piracy attack within 30 minutes of receiving a distress call.<sup>42</sup>

Another example is research using Long Range Identification and Tracking (LRIT) data to analyze the patterns of piracy on maritime routes and vessel behavior off the coast of Somalia and the High Risk Zone.<sup>43</sup> LRIT requires passenger vessels and cargo vessels of 300 gross tons or more to report their position at least four times per day, upon poll requests or automatically via satellite through the flag state's selected LRIT data center. At the height of piracy activity off Somalia and the High Risk Areas, LRIT tracking was more reliable than AIS data, as AIS data is an open-source system which pirates can also access; for this reason many shipmasters switched the system off while transiting the Somali coast. This meant that AIS tracks were incomplete in this area. LRIT contributes to creating a holistic picture when combined with other data sources.<sup>44</sup>

The 2015 study by Michele Vespe, Harm Greidanus, and Marlene Alvarez used a five-year archive of vessel positioning data to analyze changes in routes and sailing speeds. The study showed that traffic moved farther from the high-risk area to avoid piracy in 2009. After 2011, ships started moving closer to the coast as the perception of risk of piracy started to decline. Sailing speed was also reduced at the time. Sailing at higher speeds reduced the chance of being hijacked, with no vessel traveling above speeds of 18 knots being hijacked. The study found that ships were no longer traveling at 18 knots by 2013. Traveling the most direct route at lower speed can reduce the cost of fuel consumption significantly.

These are two examples of how incident data can be complemented by other forms of analysis. They reveal that incident data in its own right might not be sufficient, but that other forms of data on maritime flows can successfully complement the analysis in order to identify trends and patterns.

# DIFFERENTIATION PROBLEMS, LIMITATIONS, AND BLIND SPOTS



*U.S. Navy and Japan Maritime Self-Defense Force discuss tactical data from the combat information center during Multi Sail 2016.  
Photo: Mass Communication Specialist 2nd Class Bryan Jackson, US Navy.*

## V. DIFFERENTIATION PROBLEMS, LIMITATIONS, AND BLIND SPOTS

Quantitative analysis of piracy incidents has its limitations. Rather than basing analysis exclusively on figures, a deeper understanding of what these numbers represent and what shifts and changes are taking place is required. Southeast Asia might have a high number of small-scale theft incidents while vessels are anchored offshore or while tugboats are underway, while another region with lower numbers will experience violent attacks or kidnappings of crew.

*Primary limitations include over-reliance on quantitative data, underreporting of incidents, and disagreements over what classifies as piracy and armed robbery at sea.*

Some organizations will not report coastal incidents out of fear that doing so will inflate figures. As these incidents do not often impact the security of commercial vessels, the risk is seen as not applicable to commercial vessels, and reports are often compiled from the viewpoint of commercial companies. Where these incidents were not reported previously and are then reported, it causes a spike in statistics that is not representative of the actual situation. Even different knowledge levels and understandings of the subject matter between analysts and researchers at international organizations, security companies, and risk management companies can impact the number of incidents included in a report. Reports should clearly state what they will include and define their typologies. Analysts should aim to be consistent in their reporting.

Problems not only exist over what constitutes piracy and armed robbery at sea, but also around the willingness of countries to report incidents due to sensitivity about territorial sovereignty. For this reason, many countries are reluctant to report security incidents in their territorial waters, while they have no problem reporting safety-related incidents. In the Malacca and Singapore straits the opposite is true. For fear of foreign naval interference

in the straits, littoral states will classify piracy incidents as armed robbery.

Underreporting of piracy problems has always been a concern. Not all masters of vessels will report incidents, especially in regions such as the Gulf of Guinea and Latin America. High-risk countries will not always report because they do not want their country to be classified as such, or for insurance premiums to increase. Underreporting is especially problematic in certain categories of vessels, such as small coastal tankers and fishing vessels. Incidents involving small fishing vessels worldwide are only reported once they affect commercial vessels, otherwise it is seen as a local issue, even though it could affect commercial vessels in time.

The term “piracy” is also often used to describe a wider spectrum of maritime crime. Related activities, such as illegal fishing, oil bunkering or oil smuggling, attacks on oil rigs, and incidents relating to stowaway situations might be labeled as piracy. Incidents can also be misinterpreted as piracy when in fact they are related to drugs, fishing, or smuggling activity. It can often be impossible to determine the intended motives of maritime criminal groups, as the sailing patterns are often indistinguishable between piracy events and fishing activity, for example. It is often also problematic to differentiate between incidents of fuel smuggling and hijacking for cargo theft. Often when smugglers are intercepted by authorities, they claim to be unwilling participants and thus victims of piracy. Cases have been reported where vessels were hijacked to facilitate migrant smuggling. In these cases, it is often hard to know if the incident could in fact be classified as piracy.

Some organizations and companies also add these non-piracy-related incidents in piracy datasets, which results in elevated numbers in statistics. It is important for organizations to have a list of definitions of their criteria so researchers and analysts can interpret their reports correctly. Some terminology used by organizations can be confusing, such as the difference between robbery and theft, and requires greater clarification.

In some regions, such as the Gulf of Guinea, for example, information is available about the modus operandi during an attack, but to a large extent, there is little information in regards to what pirate networks are involved. Very few piracy suspects are arrested, and when they are,

information about individuals and pirate networks might not be available in open sources. Between 2007 and 2016, the reports of the Monitoring Group on Somalia and Eritrea pursuant to Security Council resolution 1766 (2007), 1811 (2008), 1853 (2008), 1811 (2008), and 2060 (2012) were detailed sources of information on pirate networks in Somalia. Since then, however, finding information on networks has become increasingly challenging. This type of information is occasionally available in Asia, but seldom is this the case in other regions of the world. In Asia, arrests and prosecutions of pirates and maritime criminals are more transparent and information about the network is often available on coast guard web pages or in the local media. INTERPOL has a database of pirates, but as access is limited to law enforcement personnel, how much is known on current networks is unclear. Details of court cases and prosecutions of pirates are available for Somalia, but minimal in other areas, especially Nigeria.

## VI. CONCLUSION

Today piracy is well-researched and well-documented. At least two-thirds of available incident information can be derived from data from the IMB, IMO, and ReCAAP-ISC. Incidents reported by the IMO, IMB, and ReCAAP are well-analyzed and verified by member states. Although it may seem that information from different reports confirms incidents, the source information is likely to be the same for most incidents. Incident reporting in the Gulf of Guinea and Latin America, South America, and the Caribbean is more problematic.

Maritime security companies and maritime insurers collect additional data on incidents of piracy and armed robbery as these companies are often embedded in these regions. As incidents of piracy and robbery of vessels often go unreported, it could prove helpful to make use of additional sources of information as provided by maritime security companies, maritime insurers, shipping companies, company security officers, and port officials.

Incidents on local and small vessels are often not included and are often seen as a local issue, especially when it does not affect commercial shipping at the time. Reporting companies are also aware that it might inflate statistics.

Identifying patterns and transformations of these incidents is just as important as quantifying incidents, per se. By using incident location data, researchers and analysts can capture, visualize, manipulate, and analyze spatial data in Geographic Information Systems (GIS). Data enables researchers to identify patterns and develop a predictive capability over time.

In essence, ships are beholden to the routes their cargoes must travel in order to reach their destination markets. Dangerous areas cannot always be circumvented. Dangerous and unexpected security situations must be handled. Analysis of piracy data can give us domain awareness and a predictive capability to help us manage these security risks. However, this predictive capability will be limited as long as essential elements of information, such as detailed knowledge about pirate networks, are lacking, and as long as underreporting of incidents in territorial waters and classification problems persist in reporting.

*Analysis of piracy data can give us domain awareness and a predictive capability to help us manage unavoidable security risks. However, this predictive capability will be limited as long as essential elements of information are lacking.*



*A US Navy amphibious transport dock ship deploys helicopters during a board and seizure operation by the Combined Task Force in the Gulf of Aden, 2010. Photo: Cryptologic Technician 2nd Class William Farmerie, US Navy.*

## ENDNOTES

- 1 International Chamber of Commerce's (ICC) International Maritime Bureau (IMB), <https://icc-ccs.org/>.
- 2 Author communication with Cyrus Mody, assistant director of ICC Commercial Crime Services, 6 November 2019.
- 3 ICC and IMB, "Piracy and Armed Robbery of Ships, Report for the Period 1 January to 31 December 2018," January 2019, [https://www.icc-ccs.org/reports/2018\\_Annual\\_IMB\\_Piracy\\_Report.pdf](https://www.icc-ccs.org/reports/2018_Annual_IMB_Piracy_Report.pdf).
- 4 IMO Global Integrated Shipping Information System (GISIS), <https://gisis.imo.org/Public/>.
- 5 IMO, "Piracy Reports," <http://www.imo.org/en/OurWork/Security/PiracyArmedRobbery///.aspx>.
- 6 INTERPOL, "Our 18 Databases," <https://www.interpol.int/en/How-we-work/Databases/Our-18-databases>.
- 7 INTERPOL, "Somalia: INTERPOL Member Countries Respond to Calls to Close the Net on Maritime Piracy," press release, 17 June 2009, <https://allafrica.com/stories/200906171186.html>.
- 8 INTERPOL, "Annual Report 2011."
- 9 UNODC, SHERLOC portal, <https://sherloc.unodc.org/cld/v3/sherloc/>.
- 10 ONI Shipping Threat Reports, <https://www.oni.navy.mil/News/Shipping-Threat-Reports/>.
- 11 The Anti-Shipping Activity Messages (ASAM) Database, <https://www.hsdl.org/?abstract&did=437654>.
- 12 On 26 March 2019, the product tanker Elhiblu 1 was diverted to save migrants in distress on a small boat. The migrants hijacked the vessel when they realized that the tanker was returning to Libya. Although this is a hijacking, it cannot be classified as piracy as the incident took place in international waters, which carries a two-ship requirement for the incident to be classified as piracy.
- 13 List of ReCAAP Focal Points, <https://www.recaap.org/focal-points>.
- 14 ReCAAP, "Piracy and Armed Robbery Against Ships in Asia: Annual Report 2019," <https://www.recaap.org/s//files/reports/annual/ReCAAP%20ISC%20Annual%20Report%202019.pdf>
- 15 ReCAAP online incident reporting, <http://www.recaap.org/lodge-incident-report>.
- 16 ReCAAP website, <https://www.recaap.org/focal-points>.
- 17 ReCAAP interactive map, <https://portal.recaap.org/OpenMap>.
- 18 ReCAAP, "Piracy and Armed Robbery Against Ships in Asia: Annual Report 2018," <https://criticalmaritime.eu/02/01/2018-recaap-isc-annual-report-piracy-and-armed-robbery-at-sea-declining-in-asia/>.
- 19 ReCAAP, <http://www.recaap.org/>.
- 20 Information Fusion Centre-Singapore, <https://www.ifc.org.sg>.
- 21 CRFIM, <http://crfimmadagascar.org/en/>.
- 22 Author communication with Nicolas Flury, France Liaison Officer at Madagascar IFC (Regional Maritime Information Fusion Centre) – Western Indian Ocean, 8 January 2020.
- 23 EU NAVFOR, <https://eunavfor.eu/>.
- 24 MSCHOA, <https://www.mschoa.org/>.
- 25 Ibid.
- 26 UKMTO, <https://www.ukmto.org/>.
- 27 Gayathri Iyer, "Sense for Sensibility: Maritime Domain Awareness through the Information Fusion Centre—Indian Ocean Region," Observer Research Foundation, Raisina Debates, 28 January 2020, <https://www.orfonline.org/speak/sense-for-sensibility-maritime-domain-awareness-through-the-information-fusion-centre-indian-ocean-region-ifc-ior-60811/>.
- 28 IFC-IOR, <https://www.indiannavy.nic.in/ifc-ior/>.
- 29 Author communication with Lieutenant Commander T.P. Singh, IFC-IOR, 28 January 2020.
- 30 Maritime Domain Awareness for Trade—Gulf of Guinea, <https://gog-mdat.org/>.
- 31 CARICOM IMPACS, <https://www.caricomimpacs.org>.
- 32 Lydelle Joubert, State of Piracy 2018: Assessing the Human Cost, Stable Seas, <https://stableseas.org/lications/maritime-terrorism/state-piracy-2018-human-cost>.
- 33 MAST, <https://www.mast-security.com/>.
- 34 Author communication with Jake Longworth, Senior Intelligence Analyst, EOS Risk Group, 20 January 2020.
- 35 Author communication with Freddy Furuland, Director of Security and Contingency, Intelligence and Operations Centre (IOC) at Den Norske Krigsforsikring for Skib (DNK), 16 October 2019.
- 36 Caribbean Safety and Security Net, <https://safetyandsecuritynet.org/>.
- 37 Noonsite, <https://www.noonsite.com/>.

- 38 International Maritime Organization, "Piracy and Armed Robbery Against Ships, Recommendations to Governments for Preventing and Suppressing Piracy and Armed Robbery Against Ships," MSC.1/Circ. 1333/Rev.1, 12 June 2015, <http://www.imo.org/en/OurWork/Security/SecDocs/Documents/Piracy/.1-Circ.1333-Rev.1.pdf>.
- 39 IMO, "Radiocommunications," <http://www.imo.org/en/OurWork/Safety/RadioCommunications//Pages/Default.aspx>.
- 40 Anish, "What is a Ship Security Alert System," Marine Insight, 18 October 2019, <https://www.marine.com/piracy-marine/what-is-ship-security-alert-system-ssas/>.
- 41 Lydelle Joubert, Amahlo-Suritec Piracy Report, August - October 2013, August 2014.
- 42 Matthew R. MacLeod and William M. Wardrop, "Operational Analysis at Combined Maritime Forces," 32nd International Symposium of Military Operational Research, July 2015.
- 43 Michele Vespe, Harm Greidanus, and Marlene Alvarez, "The Declining Impact of Piracy on Maritime Transport in the Indian Ocean: Statistical Analysis of 5-year Vessel Tracking Data," Marine Policy, vol. 59, September 2015, <http://www.sciencedirect.com/science/article/pii/S0308597X15001001>.
- 44 IMO, "Resolution MSC.298(87)," 21 May 2010, [http://www.imo.org/en/KnowledgeCentre/IndexofIMOfolutions/Maritime-Safety-Committee-\(MSC\)/Documents/MS.298\(87\).pdf](http://www.imo.org/en/KnowledgeCentre/IndexofIMOfolutions/Maritime-Safety-Committee-(MSC)/Documents/MS.298(87).pdf).

## SAFE SEAS

*safeseas.net* 

SafeSeas is a network of research organisations that investigate maritime security. The focus is on maritime threats and 'blue crimes', and responses in the form of law enforcement & policing, capacity building, or environmental and sustainable development.

## STABLE SEAS

*stableseas.org* 

Stable Seas, a program of One Earth Future, engages the international security community with novel research on illicit maritime activities such as piracy and armed robbery, trafficking and smuggling in persons, IUU (illegal/unregulated/unreported) fishing, and illicit trades in weapons, drugs, and other contraband. These activities perpetuate organized political violence and reinforce each other to threaten economic development and the welfare of coastal populations.

## ONE EARTH FUTURE

*oneearthfuture.org*



ONE EARTH FUTURE fosters sustainable peace by partnering with innovative world leaders, global development agencies and communities to see complex problems at the root of armed conflict in new ways and solve them together through orchestrated collaboration.

---

## CONTACT US

 [stableseas@oneearthfuture.org](mailto:stableseas@oneearthfuture.org)

---